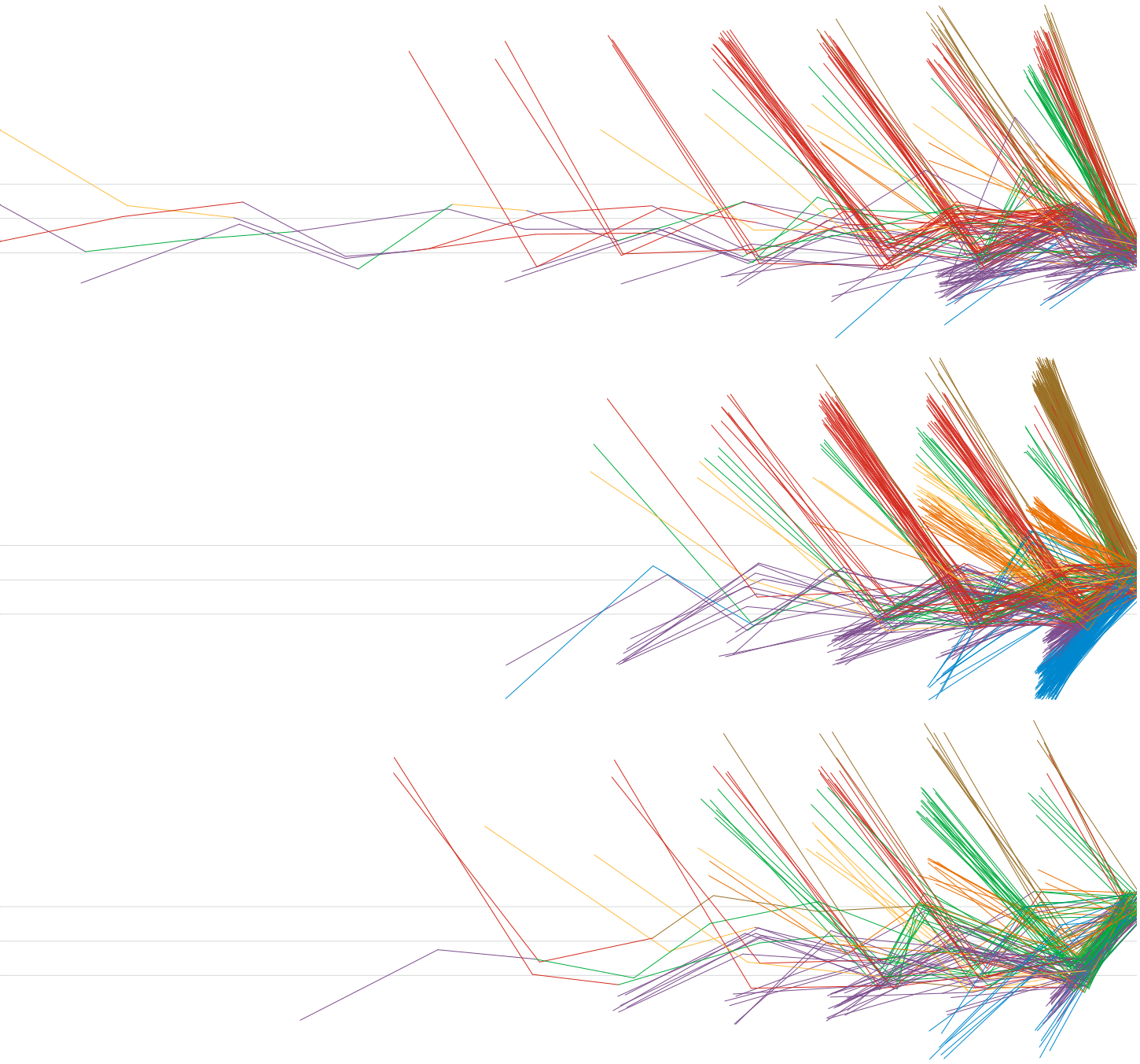
# Data Breach Investigations Report 2019

Kurzfassung



verizon

**Der Verizon Data Breach Investigations Report (DBIR) bietet Ihnen wichtige Einblicke in die Bedrohungen, denen Ihr Unternehmen potenziell ausgesetzt ist. Der 12. DBIR basiert auf 41.686 Sicherheitsvorfällen und 2.013 Datenverlusten aus der Praxis. Die Informationen wurden von 73 Datenquellen des öffentlichen und privaten Sektors aus 86 Ländern zur Verfügung gestellt.**

## Wer steckt hinter den Angriffen?

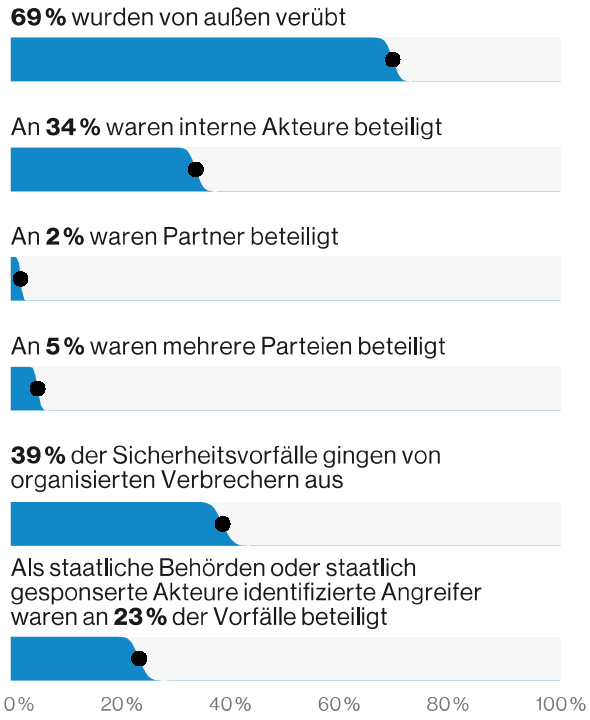



**Abbildung 1.**

## Wer sind die Opfer von Sicherheitsvorfällen?

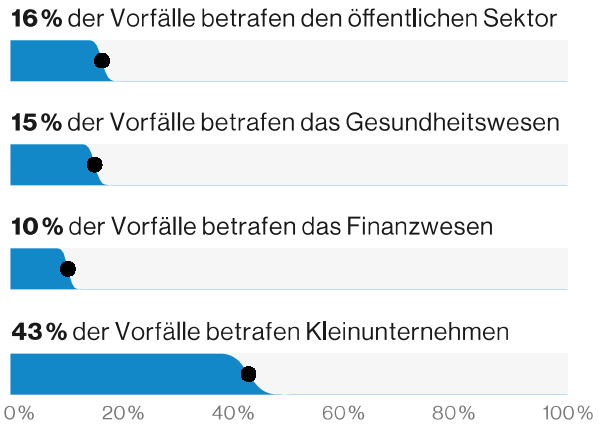



**Abbildung 2.**

## Welche Methoden werden genutzt?

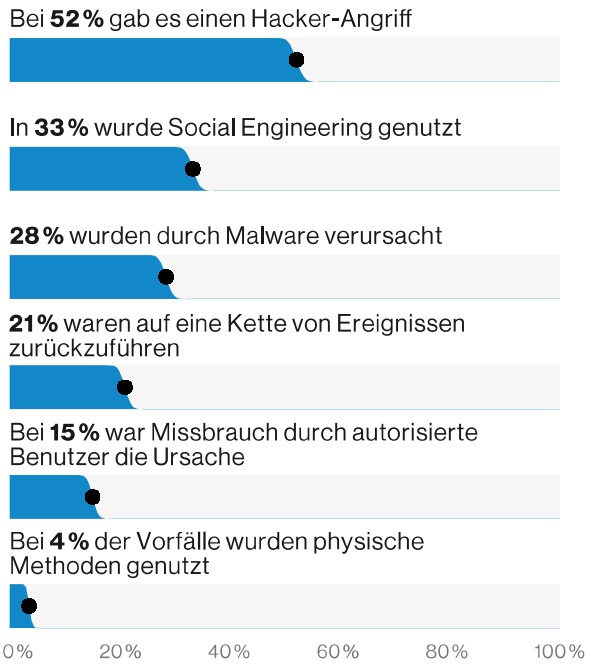



**Abbildung 3.**

Datenschutzverletzungen sorgen weiterhin weltweit für Schlagzeilen. Welche Abwehrmaßnahmen Sicherheitsexperten auch anwenden, die Angreifer scheinen stets in der Lage zu sein, diese zu umgehen. Kein Unternehmen – egal wie groß oder klein – ist davor gefeit. Keine Branche ist immun gegen Angriffe. Unabhängig von der Art oder Menge Ihrer Unternehmensdaten – irgendwo gibt es jemanden, der es darauf abgesehen hat. Doch Sie können diese Risiken effektiver und effizienter abwehren, wenn Sie über fundierte Kenntnisse der Bedrohungen verfügen, denen Sie und Ihre Mitbewerber ausgesetzt sind. Es hilft ebenfalls zu wissen, wie sich diese Bedrohungen im Laufe der Zeit weiterentwickelt haben und mit welchen Taktiken Sie voraussichtlich rechnen müssen.

# Die wichtigsten Erkenntnisse

**Angriffsziel Führungsebene**
Führungskräfte waren mit einer 12-mal so hohen Wahrscheinlichkeit von einem Social-Engineering-Vorfall betroffen und mit einer 9-mal so hohen Wahrscheinlichkeit das Opfer einer Sicherheitsverletzung durch Social Engineering als in vergangenen Jahren. Es gibt auch weitere Hinweise, dass finanziell motivierte Social-Engineering-Angriffe zunehmen. So ist die Anzahl der Sicherheitsvorfälle und Datendiebstähle, von denen Führungskräfte betroffen waren, in diesem Bericht vom einstelligen Bereich in die Dutzende gestiegen.

**Raus aus meiner Cloud**
Mit der zunehmenden Umstellung auf kostengünstigere Cloud-basierte Lösungen migrieren auch E-Mails und andere wertvolle Daten in die Cloud. Kriminelle verlagern einfach ihren Fokus und entwickeln neue Taktiken, um die für sie wertvollsten Daten zu finden und zu stehlen. Dementsprechend hat das Hacking Cloud-basierter E-Mail-Server mithilfe gestohlener Anmeldedaten zugenommen. Dies bedeutet jedoch nicht, dass Cloud-basierte Services weniger sicher sind. Phishing-Angriffe, der Diebstahl von Anmeldedaten und Konfigurationsfehler gehören hier dazu.

**Ins Netz gegangen**
Im Bereich der Zahlungskarten sind die Angriffe auf Web-Anwendungen für den elektronischen Zahlungsverkehr auf dem besten Weg, die physischen Angriffe auf Geldautomaten zu übersteigen. Gemäß den von der National Cyber-Forensics and Training Alliance (NCFTA) beigetragenen Daten scheint dieser Wandel bereits vollzogen zu sein. Auch unsere allgemeinen Daten weisen eine Tendenz in diese Richtung auf.

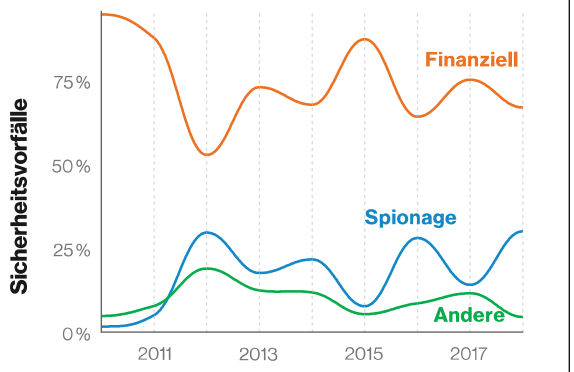



**Abbildung 7.** Motive der Angreifer – Sicherheitsvorfälle im Laufe der Zeit

Ist ein Motiv bekannt bzw. zutreffend, stellt finanzielle Bereicherung mit 71% den häufigsten Grund für eine Datensicherheitsverletzung dar. Bei 25% der Sicherheitsvorfälle ist das Motiv Spionage.

**Ransomware: nach wie vor eine Bedrohung**
Ransomware-Angriffe sind immer noch hochaktuell. So wurde bei fast 24 % der Sicherheitsvorfälle Malware genutzt. Ransomware ist mittlerweile so alltäglich geworden, dass sie in den Fachmedien kaum noch erwähnt wird – es sei denn, das Angriffsziel hat einen hohen Bekanntheitsgrad. Sie stellt jedoch nach wie vor für alle Branchen eine ernstzunehmende Bedrohung dar. Dagegen treten andere Bedrohungen, die häufig aufgebauscht werden, wie z. B. Cryptomining (2 % von Malware) gemäß unseren Daten nur sehr selten auf.

**Zahlt sich Chip & Pin aus?**
Im Bereich Zahlungskarten nehmen die physischen Angriffe auf Geldautomaten im Vergleich zur Kompromittierung von Web-Anwendungen ab. Dies könnte zum Teil auf Fortschritte bei der Implementierung von Chip & Pin-Zahlungstechnologie zurückzuführen sein.

**Die Personalabteilung schlägt zurück**
Es ist eine interessante Entwicklung, dass Angriffe auf Personalabteilungen im Vergleich zum Vorjahr abgenommen haben. Gemäß unseren Daten waren in diesem Jahr 6-mal weniger Personalmitarbeiter betroffen. Ähnlich verhält es sich mit Betrugsversuchen in Bezug auf das W-2 Formular für Steuererklärungen in den USA, für die im DBIR kaum noch Daten vorliegen.

**Ich klicke, also bin ich**
Die Klickraten bei Phishing-Simulationen für Datenpartner fielen in den vergangenen 7 Jahren von 24 % auf 3 %. 18 % der Personen, die auf einen solchen Link klickten, nutzten ein Mobilgerät. Studien zufolge sind mobile Benutzer anfälliger für Phishing-Angriffe, was vermutlich, neben anderen Faktoren, auf die Benutzeroberflächen zurückzuführen ist. Dies gilt auch für E-Mail-basierte Spear-Phishing- und Social-Media-Angriffe.

**Welchen Bedrohungen ist Ihre Branche ausgesetzt?**
Es kann jedes Unternehmen treffen. Doch manche Branchen sind anfälliger für bestimmte Arten von Angriffen als andere. Dabei spielen zahlreiche Faktoren eine Rolle, wie z. B. das Geschäftsmodell, die Art der übertragenen und gespeicherten Daten, der Kundenstamm und selbst die verschiedenen Technologien, die zur Sicherung der Umgebung erforderlich sind. Wenn Sie wissen, wo ein Angriff am wahrscheinlichsten ist, haben Sie die Möglichkeit, den Einsatz Ihrer Ressourcen zu optimieren und Budgets entsprechend zuzuweisen.

Viele Leser des DBIR blättern direkt zu den Informationen über ihre eigene Branche, um die Bedrohungen zu verstehen, denen sie und ihre Mitbewerber ausgesetzt sind. Doch Sie können auch aus den Erfahrungen anderer Branchen wertvolle Einblicke gewinnen.

**Der DBIR 2019 beschäftigt sich intensiv mit verschiedensten Branchen und geht auf die spezifischen Bedrohungen, Motive und Angreifer ein.**

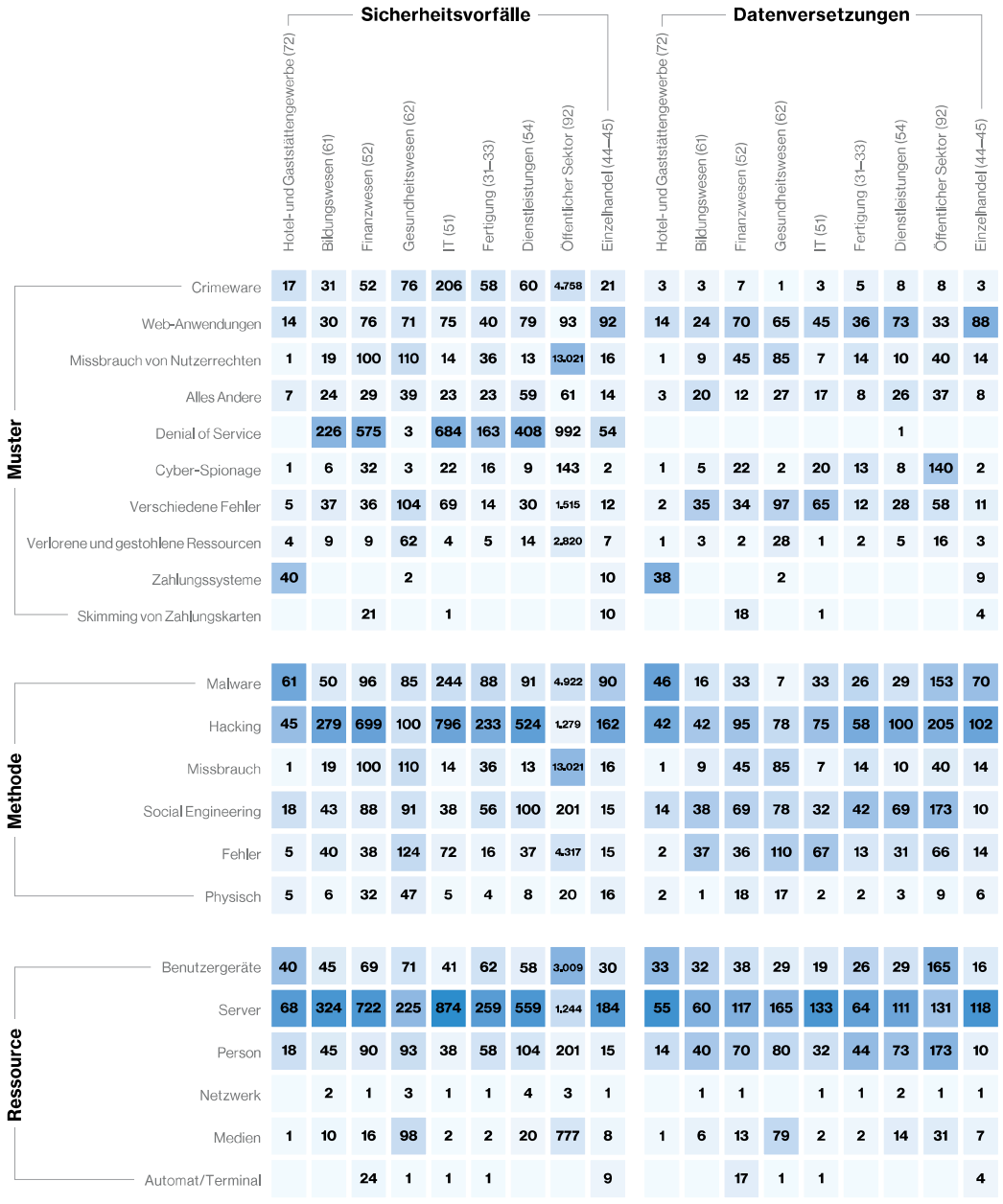



**Abbildung 39.** Branchenvergleich
(links: alle Sicherheitsvorfälle, rechts: nur Datenverletzungen)

## Hotel- und Gaststättengewerbe HoH

**Gemäß unseren Daten haben hier die Sicherheitsvorfälle gegenüber dem Vorjahr abgenommen. Dies ist vor allem auf eine geringere Anzahl an Vorfällen bei PoS-Anbietern zurückzuführen, die in der Vergangenheit dazu führten, dass zahlreiche Unternehmen mit den gestohlenen Anmeldedaten von Partnern geschädigt wurden.**

| | |
|---|---|
| **Häufigkeit** | 87 Vorfälle, davon 61 mit bestätigter Offenlegung von Daten |
| **Top 3 Muster** | PoS-Systemangriffe, Web-Anwendungen und Crimeware stellen 93% aller Vorfälle im Hotel- und Gaststättengewerbe dar |
| **Angreifer** | Extern (95%), intern (5%) (Sicherheitsvorfälle) |
| **Motive** | Finanziell (100%) (Sicherheitsvorfälle) |
| **Kompromittierte Daten** | Zahlungsdaten (77%), Anmeldedaten (25%), intern (19%) (Sicherheitsvorfälle) |

## Bildungswesen

**Das Bildungswesen hat nach wie vor mit Fehlern, Social Engineering und unzureichender Sicherung von E-Mail-Anmeldedaten zu kämpfen. Mehr als die Hälfte der Vorfälle sind auf DoS-Angriffe zurückzuführen.**

| | |
|---|---|
| **Häufigkeit** | 382 Vorfälle, davon 99 mit bestätigter Offenlegung von Daten |
| **3 MusterTop** | Verschiedenste Fehler, Web-Anwendungen und „Alles Andere“ stellten 80% der Sicherheitsvorfälle dar |
| **Angreifer** | Extern (57%), intern (45%), mehrere Parteien (2%) (Sicherheitsvorfälle) |
| **Motive** | Finanziell (80%), Spionage (11%), Spaß (4%), Frustration (2%), Ideologie (2%) (Sicherheitsvorfälle) |
| **Kompromittierte Daten** | Personenbezogen (55%), Anmeldedaten (53%), intern (35%) (Sicherheitsvorfälle) |

## Finanz- und Versicherungswesen

**Denial-of-Service-Angriffe (DoS) und die Verwendung gestohlener Anmeldedaten in Banking-Anwendungen sind nach wie vor üblich. Durch Filterprozesse kann geklärt werden, welche E-Mail-Konten kompromittiert sind. Skimming an Geldautomaten ist weiterhin rückläufig.**

| | |
|---|---|
| **Häufigkeit** | 927 Vorfälle, davon 207 mit bestätigter Offenlegung von Daten |
| **Top 3 Muster** | Webanwendungen, Missbrauch von Nutzerrechten und sonstige Fehler stellen 72% der Sicherheitsvorfälle dar |
| **Angreifer** | Extern (72%), intern (36%), mehrere Parteien (10%), Partner (2%) (Sicherheitsvorfälle) |
| **Motive** | Finanziell (88%), Spionage (10%) (Sicherheitsvorfälle) |
| **Kompromittierte Daten** | Personenbezogen (43%), Anmeldedaten (38%), intern (38%) (Sicherheitsvorfälle) |

## Gesundheitswesen

**Auffällig am Gesundheitswesen ist, dass die Mehrheit der Sicherheitsvorfälle von internen Angreifern verursacht wird. DoS-Angriffe sind selten, es kann jedoch aufgrund von Ransomware zu Verfügbarkeitsproblemen kommen.**

| | |
|---|---|
| **Häufigkeit** | 466 Vorfälle, davon 304 mit bestätigter Offenlegung von Daten |
| **Top 3 Muster** | Verschiedenste Fehler, Missbrauch von Nutzerrechten und Web-Anwendungen stellen 81% der Vorfälle im Gesundheitswesen dar |
| **Angreifer** | Intern (59%), extern (42%), Partner (4%), mehrere Parteien (3%) (Sicherheitsvorfälle) |
| **Motive** | Finanziell (83%), Spaß (6%), Bequemlichkeit (3%), Frustration (3%), Spionage (2%) (Sicherheitsvorfälle) |
| **Kompromittierte Daten** | Medizinisch (72%), personenbezogen (34%), Anmeldedaten (25%) (Sicherheitsvorfälle) |

## IT-Branche

**Web-Anwendungen sind durch Angriffe auf deren Verfügbarkeit und damit auch für Attacken auf Cloud-basierte E-Mail-Konten betroffen.**

| | |
|---|---|
| **Häufigkeit** | 1.094 Vorfälle, davon 155 mit bestätigter Offenlegung von Daten |
| **Top 3 Muster** | Verschiedenste Fehler, Web-Anwendungen und Cyber-Spionage stellen 83% der Sicherheitsvorfälle im IT-Bereich dar |
| **Angreifer** | Extern (56%), intern (44%), Partner (2%) (Sicherheitsvorfälle) |
| **Motive** | Finanziell (67%), Spionage (29%) (Sicherheitsvorfälle) |
| **Kompromittierte Daten** | Personenbezogen (47%), Anmeldedaten (34%), Geschäftsgeheimnisse (22%) (Sicherheitsvorfälle) |

## Fertigung

**In der Fertigungsbranche war in den vergangenen Jahren eine Zunahme der finanziell motivierten Sicherheitsvorfälle zu beobachten. Doch auch Spionage bleibt ein wichtiges Motiv. Die meisten Sicherheitsvorfälle waren mit Phishing und der Nutzung von gestohlenen Anmeldedaten verbunden.**

| | |
|---|---|
| **Häufigkeit** | 352 Vorfälle, davon 87 mit bestätigter Offenlegung von Daten |
| **Top 3 Muster** | Web-Anwendungen, Missbrauch von Nutzerrechten und Cyber-Spionage stellen 71% der Sicherheitsvorfälle dar |
| **Angreifer** | Extern (75%), intern (30%), mehrere Parteien (6%), Partner (1%) (Sicherheitsvorfälle) |
| **Motive** | Finanziell (68%), Spionage (27%), Frustration (3%), Spaß (2%) (Sicherheitsvorfälle) |
| **Kompromittierte Daten** | Anmeldedaten (49%), intern (41%), Geschäftsgeheimnisse (36%) (Sicherheitsvorfälle) |

## Professionelle, technische und wissenschaftliche Dienstleistungen

**In dieser Branche sind Phishing und der Diebstahl von Anmeldedaten in Verbindung mit Cloud-basierten E-Mail-Konten mittlerweile die vorherrschenden Angriffsarten.**

| | |
|---|---|
| **Häufigkeit** | 670 Vorfälle, davon 157 mit bestätigter Offenlegung von Daten |
| **Top 3 Muster** | Web-Anwendungen, „Alles Andere“ und verschiedene Fehler stellen 81% der Sicherheitsvorfälle dar |
| **Angreifer** | Extern (77%), intern (21%), Partner (5%), mehrere Parteien (3%) (Sicherheitsvorfälle) |
| **Motive** | Finanziell (88%), Spionage (14%), Bequemlichkeit (2%) (Sicherheitsvorfälle) |
| **Kompromittierte Daten** | Anmeldedaten (50%), intern (50%), personenbezogen (46%) (Sicherheitsvorfälle) |

## Öffentlicher Sektor

**Cyber-Spionage ist im öffentlichen Sektor ein sehr wichtiges Thema. Dabei sind staatlich gesponserte Akteure für 79% aller Sicherheitsvorfälle verantwortlich, die von externen Angreifern ausgingen. 30% der Sicherheitsvorfälle sind auf den Missbrauch von Nutzerrechten und Fehler durch Insider zurückzuführen.**

| | |
|---|---|
| **Häufigkeit** | 23.399 Vorfälle, davon 330 mit bestätigter Offenlegung von Daten |
| **Top 3 Muster** | Cyber-Spionage, verschiedenste Fehler und Missbrauch von Nutzerrechten stellen 72% der Vorfälle dar |
| **Angreifer** | Extern (75%), intern (30%), Partner (1%), mehrere Parteien (6%) (Sicherheitsvorfälle) |
| **Motive** | Spionage (66%), finanziell (29%), andere (2%) (Sicherheitsvorfälle) |
| **Kompromittierte Daten** | Intern (68%), personenbezogen (22%), Anmeldedaten (12%)(Sicherheitsvorfälle) |

## Einzelhandel

**Bei Transaktionen mit Zahlungskarte sind PoS-Angriffe oder das Ablesen von Kartendaten (Skimming) weiterhin rückläufig. In dieser Branche konzentrieren sich die Angreifer vorwiegend auf Online-Zahlungsanwendungen, um sich finanziell zu bereichern.**

| | |
|---|---|
| **Häufigkeit** | 234 Vorfälle, davon 139 mit bestätigter Offenlegung von Daten |
| **Top 3 Muster** | Web-Anwendungen, Missbrauch von Nutzerrechten und verschiedenste Fehler stellen 81% der Sicherheitsvorfälle dar |
| **Angreifer** | Extern (81%), intern (19%) (Sicherheitsvorfälle) |
| **Motive** | Finanziell (97%), Spaß (2%), Spionage (2%) (Sicherheitsvorfälle) |
| **Kompromittierte Daten** | Zahlungsdaten (64%), Anmeldedaten (20%), personenbezogen (16%) (Sicherheitsvorfälle) |

# Nutzen Sie praxisbezogene Informationen für Ihre Sicherheit

Sicherheitsbedrohungen und Angriffsmethoden entwickeln sich ständig weiter und IT-Sicherheitsexperten haben möglicherweise manchmal das Gefühl, dass sie mit den Angreifern nicht mehr Schritt halten können. Doch Sicherheitsexperten und Führungskräfte haben ihre eigenen leistungsfähigen Tools, die sie gegen Kriminelle nutzen können.

Ihre beste Verteidigung ist Wissen. Neue Perspektiven und Einsichten werden Ihnen helfen, Bedrohungen zu erkennen und außerdem zu verstehen, welche wirksamen Gegenmaßnahmen Sie ergreifen können. Der DBIR spielt eine wichtige Rolle, weil er aktuellste Erkenntnisse enthält. Seit 2014 haben wir neun Angriffsmuster identifiziert, die auch heute noch den Großteil der Datenschutzverletzungen und Sicherheitsvorfälle abdecken. Wenn Sie diese Muster kennen, können Sie Ihre Sicherheitsmethoden besser konfigurieren und Ihr Budget so planen, dass Sie optimal auf potenzielle Bedrohungen vorbereitet sind.

> **98 % der Sicherheitsvorfälle und 88 % der Datenverluste entsprechen weiterhin einem dieser neun Muster.**

Für Unternehmen steht viel auf dem Spiel, denn ihr Kundenstamm, ihre geschützten Geschäftsdaten und ihre Betriebsgeheimnisse sind für Angriffe anfällig. Datenschutzverletzungen bedrohen weiterhin die Reputation, die Finanzen und das Bestehen von Unternehmen. Aber Sicherheitsexperten haben die Macht, diese Herausforderungen zu meistern.

Im DBIR 2019 finden Sie sämtliche Details, einschließlich branchenspezifischer Angriffsmuster.

> **Eine Schadensbilanz**
>
> **Das Internet Crime Complaint Center (IC3) des FBI hat dieses Jahr am DBIR mitgewirkt und Daten zu den Auswirkungen der Kompromittierung von Geschäfts-E-Mails (Business Email Compromise, BEC) und des Diebstahls von Computerdaten (Computer Data Breach, CDB) zur Verfügung gestellt. Bei BECs belaufen sich die durchschnittlichen Verluste, die durch Angreifer verursacht wurden, auf rund 8.000 USD; bei CDBs auf rund 25.000 USD.**
>
> **Großer Einsatz für Ihr Geld**
>
> **Als das IC3 Recovery Asset Team in Zusammenarbeit mit den betroffenen Banken bei BECs tätig wurde, konnte bei der Hälfte aller in den USA ansässigen BEC-Opfer 99 % des Geldes wieder zurückgewonnen oder eingefroren werden. Nur 9 % konnten nichts zurückerhalten.**

### Hier einige Tipps, um Sicherheitsvorfälle zu verhindern

**Ordnung muss sein.**
Viele Sicherheitsvorfälle sind das Ergebnis von unzureichenden Sicherheitsstandards und mangelnder Detailgenauigkeit. Soweit möglich, schließen Sie menschliches Versagen aus und legen Sie dann eine Ausgangsbasis zur Sicherung Ihrer Internetanbindungen, z. B. für Webserver und Cloud-Services, fest.

**Bewahren Sie Integrität.**
Angriffe auf Web-Anwendungen beinhalten heute Code, der in Web-Formulare eingegebene Daten abgreifen kann. Erwägen Sie den Einsatz von FIM (File Integrity Monitoring – Überwachung der Datenintegrität) auf Zahlungswebseiten, verwenden Sie Patches für Betriebssysteme und nutzen Sie codierte Zahlungsanwendungen.

**Doppelt hält besser.**
Setzen Sie auf Zwei-Faktor-Authentifizierung (2FA). Nutzen Sie starke Authentifizierungsprozesse für Kundenanwendungen, jeglichen Fernzugriff und Cloud-basierte E-Mail-Services. Auch wenn 2FA Schwachstellen haben kann, ist dies kein Grund, auf ihre Implementierung zu verzichten.

**Die Gefahr lauert im Inneren.**
Verfolgen Sie das Verhalten von Insidern, indem Sie den Zugriff auf sensible Daten überwachen und penibel protokollieren. Machen Sie Ihren Mitarbeitern klar, wie gut Sie darin sind, betrügerische Transaktionen zu erkennen.

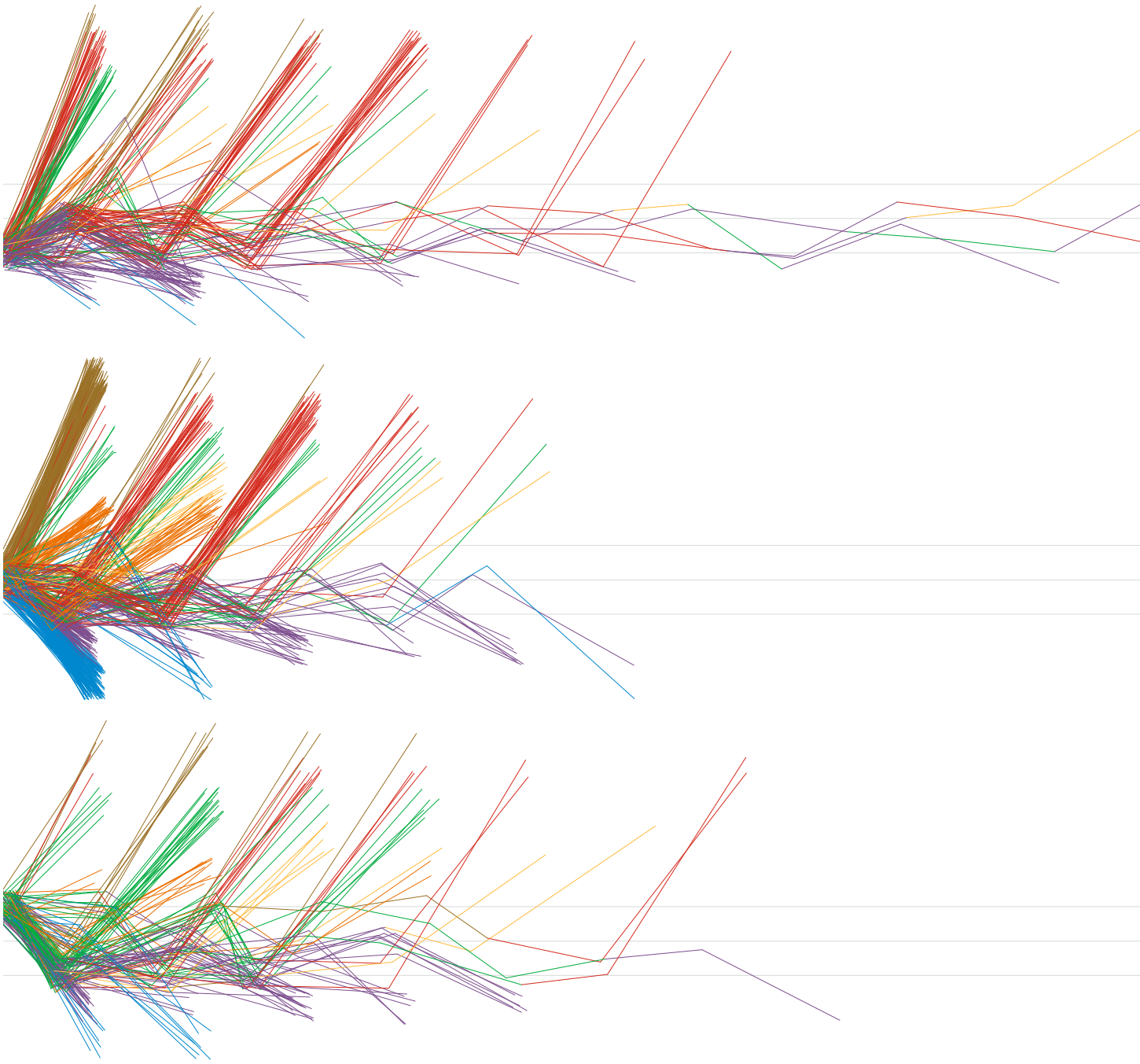
**Überwachen Sie den Datenverkehr.**
Der Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) ist für viele Branchen eine essenzielle Kontrollmaßnahme. Verhindern Sie nicht bösartige Unterbrechungen durch kontinuierliche Überwachung und Kapazitätsplanung für Datenverkehrsspitzen.

**Entwickeln Sie soziales Bewusstsein.**
Social-Engineering-Angriffe stellen eine effektive Möglichkeit dar, um an Anmeldedaten zu gelangen. Überprüfen Sie Links und ausführbare Dateien in Ihren E-Mails. Geben Sie Ihren Teams die Möglichkeit, potenzielle Phishing- und Pretexting-Attacken zu melden.

Der Verizon Data Breach Investigations Report 2019 bietet Sicherheitsexperten und Führungskräften weltweit einen umfassenden Überblick über die aktuelle Bedrohungslandschaft. Dabei zeigt er auf, wie sich diese Gefahren weiterentwickeln und stellt neueste Verfahren zur Minderung der Risiken vor. Der Bericht von 2019 beruht auf der detaillierten Analyse von 41.686 Sicherheitsvorfällen, einschließlich 2.013 bestätigten Datenschutzverletzungen. Der DBIR erscheint bereits seit 12 Jahren und gilt als eine der renommiertesten Quellen der Sicherheitsbranche.

**Laden Sie den vollständigen Bericht herunter:**
enterprise.verizon.com/DBIR2019/

# Data Breach Investigations Report 2019 Kurzfassung



verizon