

# Informationen, mit denen Sie sich wappnen können

Die wichtigsten Zahlen und Fakten aus dem Verizon Data Breach Investigations Report 2022

2008 2022

Seit 15 Jahren dokumentiert und klassifiziert Verizon Sicherheitsverletzungen. Die diesjährige Ausgabe des DBIR stützt sich auf:

**5.212**

analysierte Datenlecks

**23.896**

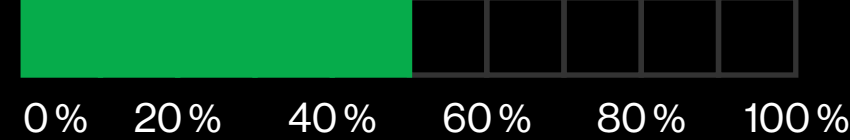
untersuchte Sicherheitsvorfälle

**87**

Unternehmen stellten Daten zur Verfügung

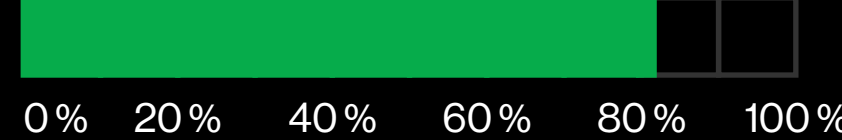
## Unsere Erkenntnisse:

**> 50 %**



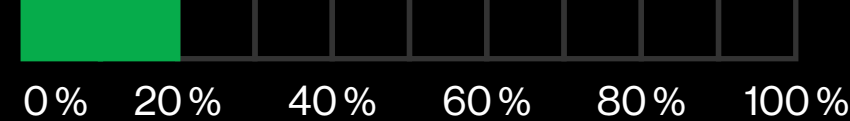
der Verstöße wurden über Remote Access oder Web-Applikationen verübt

**82 %**



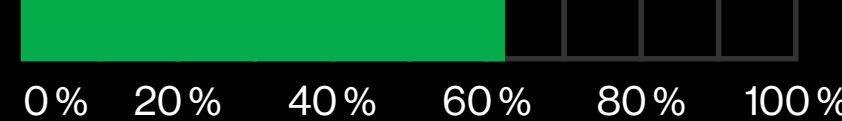
der erfassten Sicherheitsverletzungen wurde durch menschliches Zutun ermöglicht

**20 %**



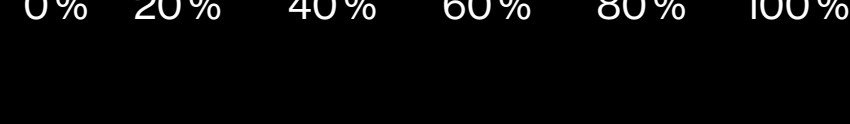
der Sicherheitsverletzungen wurde durch Ransomware verursacht

**62 %**



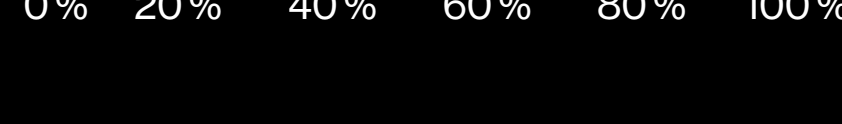
der Systeminfiltrationen erfolgten über Partnerunternehmen, meist durch einen erfolgreichen Hackerangriff auf eine bestimmte Lieferkette

**66 %**



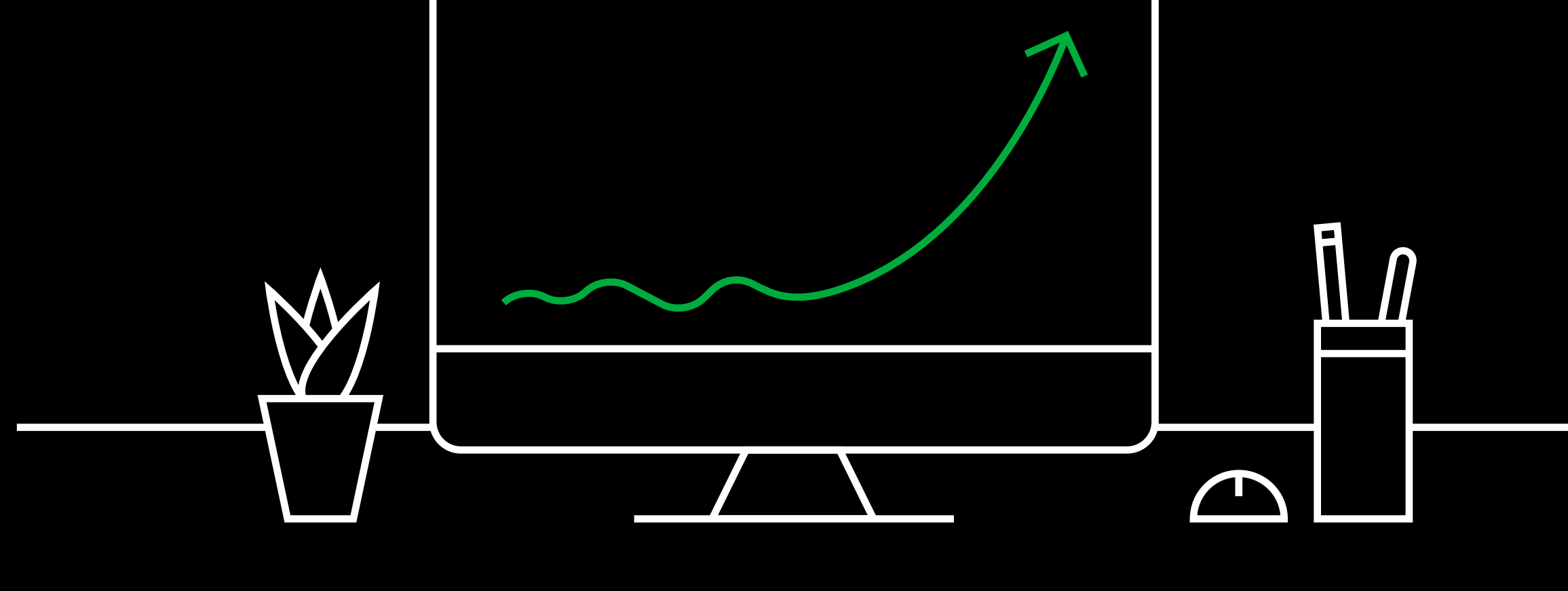
wurden durch Phishing, gestohlene Anmeldedaten und/oder Ransomware verursacht

**95 %**

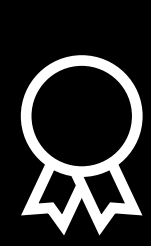


der erfolgreichen Angriffe umfassten maximal fünf Schritte

Ransomware ist im vergangenen Jahr um **13 %** gestiegen – mehr als in den letzten fünf Jahren zusammengenommen



## Die vier wichtigsten Angriffswege:



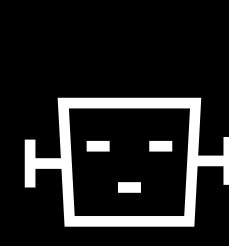
Zugangsdaten



Phishing



Ausnutzung von Schwachstellen



Botnets

Kein Unternehmen ist sicher, wenn es nicht mit diesen Angriffen umgehen kann

## Wer sind die Täter?

**4/5**

Sicherheitsverletzungen gehen auf das Konto organisierter Krimineller

**#1**

Auf Platz Eins der Motive: Finanzielle Vorteile

**#2**

Auf Platz Zwei: Spionage

Die Sicherheit Ihres Unternehmens ist entscheidend. Der Verizon DBIR 2022 ist der richtige Ort, um damit zu beginnen.

Hier finden Sie außerdem detaillierte Analysen der neuesten Bedrohungen sowie spezifische Informationen und Statistiken für 12 Branchen und vier Regionen.

[Zum Download](#)

verizon