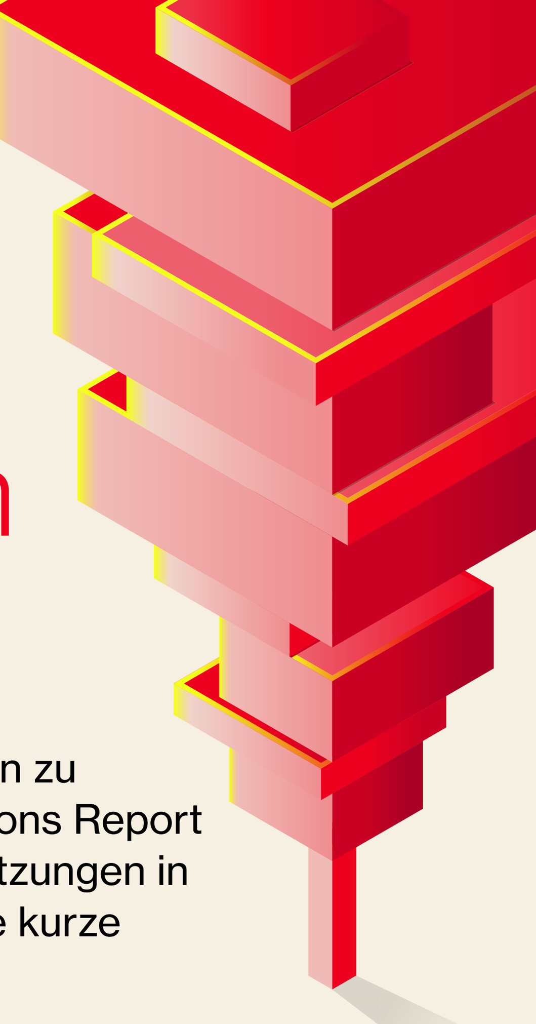
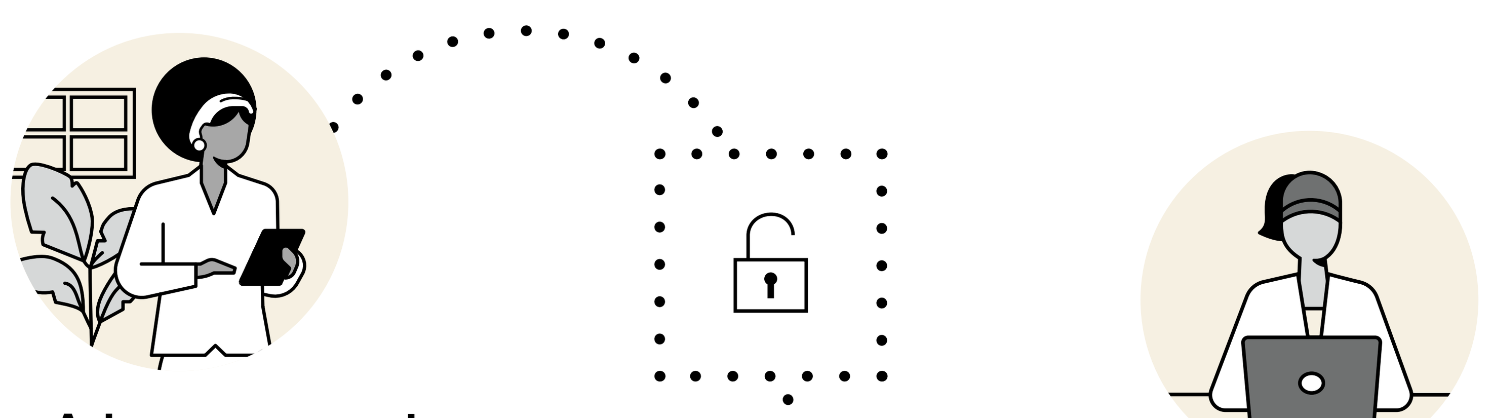
Lassen Sie Angriffe am Bollwerk Ihrer Cybersicherheits-kenntnisse abprallen



Data Breach Investigations Report 2025: das Wichtigste in Kürze

Es ist an der Zeit, ein Licht auf zwielichtige Aktivitäten zu werfen. Für den diesjährigen Data Breach Investigations Report (DBIR 2025) haben wir 12.195 Datensicherheitsverletzungen in 139 Ländern analysiert. Im Folgenden finden Sie eine kurze Übersicht über die wichtigsten Ergebnisse.



Ahnungslose Komplizen?

15 % → 30 %

Der Anteil der Sicherheitsverstöße, bei denen eine dritte Partei involviert war, hat sich seit dem letzten Bericht verdoppelt. Das zeigt, wie wichtig die sorgfältige Auswahl der richtigen Partner und Zulieferer ist.

Wenn Sie, Ihre Partner und Zulieferer Ihr Cybersicherheits-niveau gemeinsam stärken und vereinheitlichen, sind Sie alle weniger anfällig.

Wissen Sie, wo Ihre Schwachpunkte sind? Ihre Gegner schon.

34 % ↑

Der Anteil der Vorfälle, bei denen Angreifer sich durch die Ausnutzung von Schwachstellen Zugang verschafften, stieg um 34 % auf 20 % aller bestätigten Sicherheitsverletzungen an.

Cyberkriminelle hoffen auf Verzögerungen

32 Tage

Unsere Analyse zeigt, dass nur 54 % der Sicherheitslücken in Geräten am Unternehmens-perimeter vollständig behoben wurden und dass dies im Median 32 Tage dauerte.

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	+1			

Mehr Ransomware-Angriffe

44 %

der Cybersicherheitsverletzungen hatten eine Ransomware-Komponente, im vorigen Berichtszeitraum waren es 37 %.

„Geld her oder ..."

115.000 USD

Ransomware-Angriffe können teuer werden. Der Medianwert der gezahlten Lösegelder lag bei 115.000 USD.

Die gute Nachricht ist: Die Mehrheit der betroffenen Unternehmen – 64 % – zahlten das geforderte Lösegeld nicht.

Was haben die meisten Datensicherheitsverletzungen gemeinsam? Den Faktor Mensch.

60 %

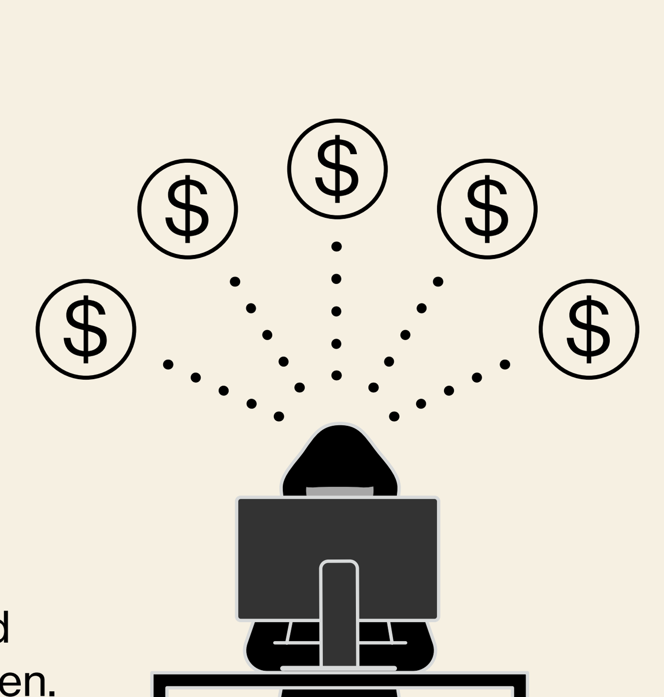
der Sicherheitsverletzungen wurden durch menschliche Fehler begünstigt – derselbe Anteil wie im Vorjahresbericht.

Der Missbrauch von Anmeldedaten und Social Engineering (wie z. B. Phishing) spielten bei diesen Vorfällen eine große Rolle.

Raub im Staatsauftrag

28 %

17 % der Sicherheitsverstöße sind Spionageangriffe. Doch damit geben staatlich gesponserte Angreifer – und ihre Auftraggeber – sich nicht zufrieden. 28 % ihrer Angriffe waren finanziell motiviert.



Kein Gerät ist immun

30 % verwaltete Geräte

46 % verwaltete Geräte

Unsere Analyse der Anmeldedaten-Logs der Infostealer-Malware ergab, dass 30 % der infiltrierten Systeme von Unternehmen lizenzierte Geräte waren. 46 % der Geräte, von denen Anmeldedaten für Unternehmenssysteme gestohlen wurden, erwiesen sich als nicht verwaltete (also private) Geräte oder Geräte, die unter Missachtung der Unternehmensrichtlinien genutzt wurden.

Auch Bots mischen mit

200 %

Cyberangriffe werden nachweisbar durch KI verstärkt. Die Anzahl der schädlichen E-Mails mit synthetisch erzeugtem Text hat sich im Verlauf der letzten zwei Jahre verdoppelt.

Wissen Sie, was Ihre Mitarbeitenden an GenAI verraten?

15 %

der Angestellten greifen routinemäßig von Unternehmens-geräten aus auf GenAI-Plattformen zu – und steigern damit das Risiko eines Datenlecks.

Holen Sie sich den umfassendsten und renommiertesten Bericht zu Cybersicherheitsverstößen: DBIR.

Wenn Sie wissen, welche Taktiken Hacker oft nutzen, können Sie die Systeme Ihres Unternehmens besser schützen. Gehen Sie den ersten Schritt zu einem höheren Sicherheitsniveau: Lesen Sie den Data Breach Investigations Report 2025.

Kontaktieren Sie Ihren Ansprechpartner bei Verizon, um herauszu-finden, wie unser erfahrenes Team Ihr Unternehmen beim Kampf gegen immer neue Cyberbedrohungen unterstützen kann. Gemeinsam können wir Ihre Daten vor zwielichtigen Aktivitäten schützen.

Lesen Sie den Bericht unter verizon.com/dbir.

verizon business