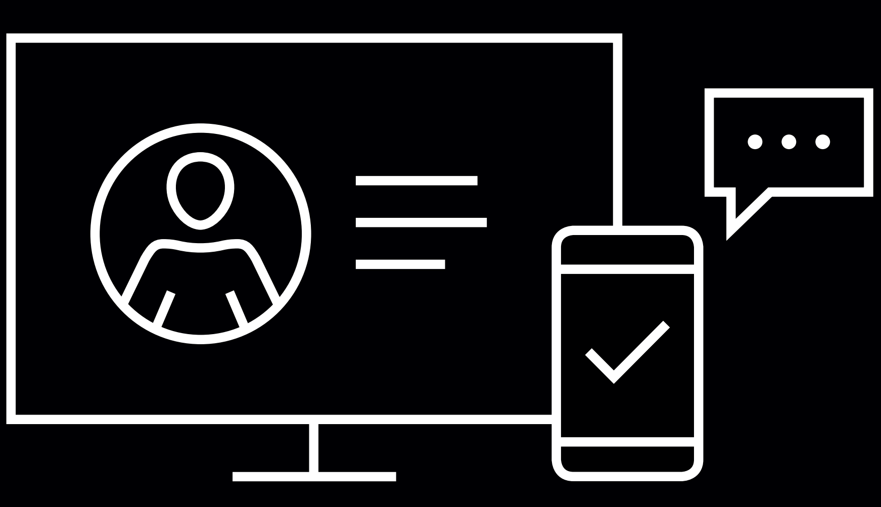
Umfassend. Fundiert. Renommiert.

Sieben wichtige Ergebnisse aus dem Verizon Data Breach Investigations Report 2023

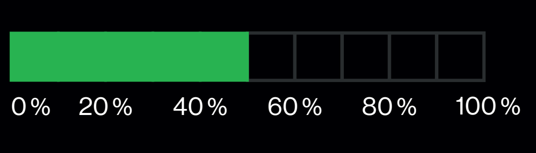
Cyberkriminelle wollen Daten stehlen und nehmen Unternehmen wie Ihres dazu mit unterschiedlichen Angriffsarten ins Visier.

Das ist das unmissverständliche Ergebnis der Zusammenfassung und Analyse der diesbezüglichen Trends des vergangenen Jahres im Data Breach Investigations Report 2023. Die Autoren betrachten die häufigsten, gefährlichsten und am schnellsten zunehmenden Angriffsmuster detailliert und gelegentlich mit einer Prise Humor, um Unternehmen in aller Welt auf sie vorzubereiten.



Mehr Pretexting

50 %

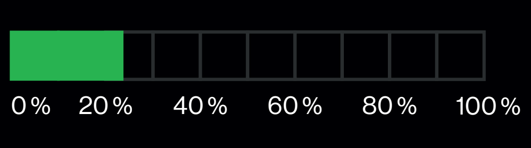


Bei 50 % der Social-Engineering-Angriffe des Jahres 2022 erfanden die Angreifer einen speziellen Vorwand – einen sogenannten Pretext –, um die Opfer zur Preisgabe von Informationen oder zu Aktionen zu bewegen, die ihrem Angriff Vorschub leisteten.

„Wir haben eure Daten. Geld her.“

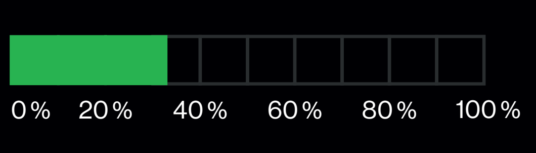
Bei 24 % der Angriffe war Ransomware (die böswillige Verschlüsselung von Daten gefolgt von Lösegeldforderungen für die Entschlüsselung oder Rückgabe) im Einsatz. Über 62 % der durch organisierte Kriminelle verursachten und 59 % der finanziell motivierten Vorfälle fielen in diese Kategorie.

24 %



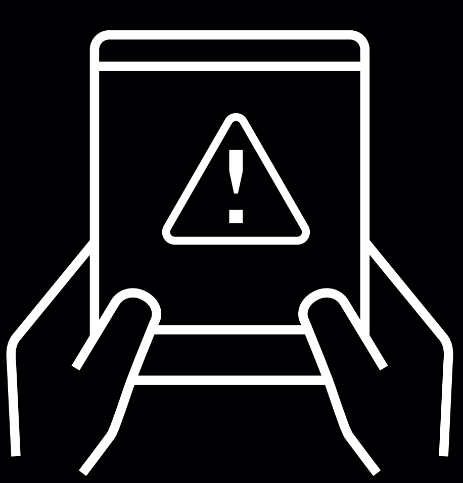
Schnellere Umsetzung

>32 %



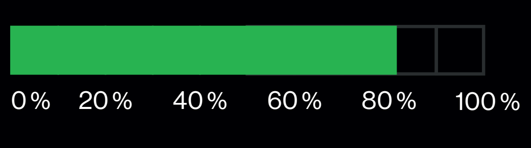
Über 32 % der Suchen nach der Log4j-Schwachstelle in diesem weit verbreiteten Java-Dienst (über die Hacker Server unter ihre Kontrolle bringen können) fanden in den ersten 30 Tagen nach deren Veröffentlichung statt.

Das zeigt, wie schnell eine Bedrohung zu einer realen, allgegenwärtigen Gefahr werden kann.



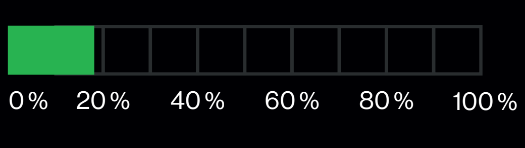
Die meisten Bedrohungen kommen von außen. Insider können jedoch ebenso gefährlich sein.

83 %



83 % der Angriffe gingen von externen Akteuren, meist finanziell motivierten Hackergruppen, aus.

19 %

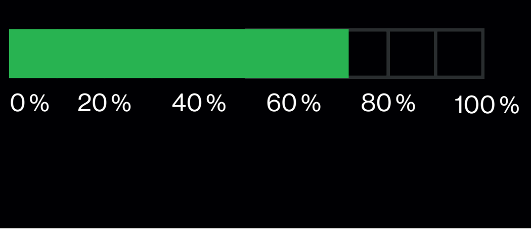


An 19 % waren Insider entweder mutwillig oder versehentlich (durch Missbrauch oder ganz gewöhnliche Fehler) beteiligt.

Menschliche Schwächen

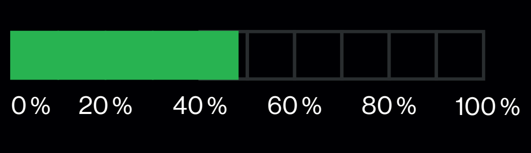
Bei 74 % der Angriffe wurden Bedienfehler, der Missbrauch von Nutzerrechten, gestohlene Anmeldedaten, Social Engineering oder Ähnliches ausgenutzt.

74 %



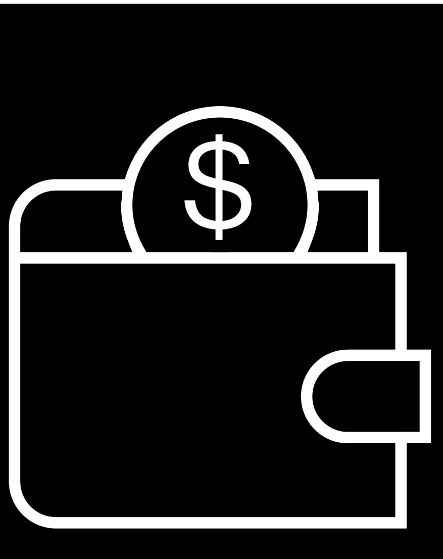
Hacker sind clever, hartnäckig und zu oft erfolgreich

49 %



Bei 49 % der externen Angriffe wurden gestohlene Anmeldedaten genutzt. Phishing machte 12 % der externen Angriffe aus. In 5 % der Angriffe wurden Schwachstellen ausgenutzt.

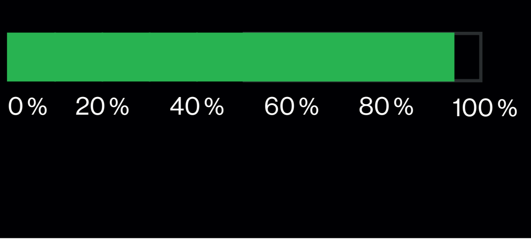
Sie müssen also auf diverse Taktiken vorbereitet sein.



Die Motivation ist allerdings (fast) immer dieselbe: Geld.

95 % aller Angriffe sind finanziell motiviert.

95 %



Der Schutz Ihrer Organisation beginnt mit einem guten Verständnis der relevanten Bedrohungen. Mit einer schnelleren Angriffserkennung können Sie Hackern sehr viel effektiver Paroli bieten.

Lesen Sie den ganzen Data Breach Investigations Report 2023 von Verizon (auf Englisch), um sich umfassend zu informieren. Sprechen Sie anschließend mit Ihrem Verizon-Vertreter vor Ort darüber, wie Verizon Sie beim Härten Ihrer Infrastruktur unterstützen kann.

Lesen Sie den Bericht unter verizon.com/dbir.

verizon