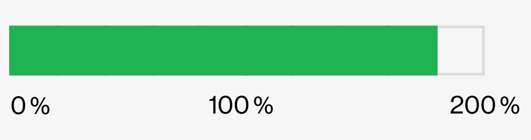
Unsere Daten zeigen, wie sie eindringen

Wichtige Ergebnisse des Data Breach Investigations Report 2024 von Verizon

2023 war ein gutes Jahr für Cyberkriminelle. Wie der Data Breach Investigations Report 2024 von Verizon aufzeigt, richtete eine Rekordzahl an Sicherheitsvorfällen – mehr als 10.000 – in 94 Ländern Schaden an. Wir haben diese Vorfälle verfolgt und analysiert, um Trends in den Angriffsmustern zu dokumentieren und Ihnen die Informationen an die Hand zu geben, die Sie angesichts der dynamischen Bedrohungslandschaft benötigen. Im Folgenden finden Sie einige wichtige Ergebnisse.

Schwächen werden ausgenutzt.

180 %



Die Ausnutzung von Schwachstellen als Einfallstor ist um 180 % – und damit fast dreimal so stark wie im vergangenen Jahr – gestiegen. Dies ist zum Teil auf die MOVEit-Sicherheitslücke und diverse von Ransomware-Angreifern genutzte Zero-Day-Exploits zurückzuführen.

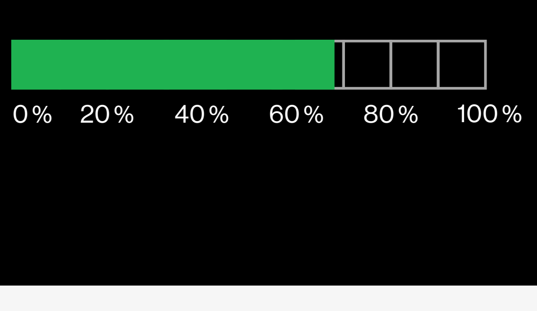
Sicherheitsteams müssen schneller reagieren.

Patches für 50 % der kritischen Sicherheitslücken werden erst etwa 55 Tage nach ihrer Veröffentlichung eingespielt. Diese Verzögerung ist gefährlich.

55 Tage

Mehr Schulungen sind nötig.

68 %

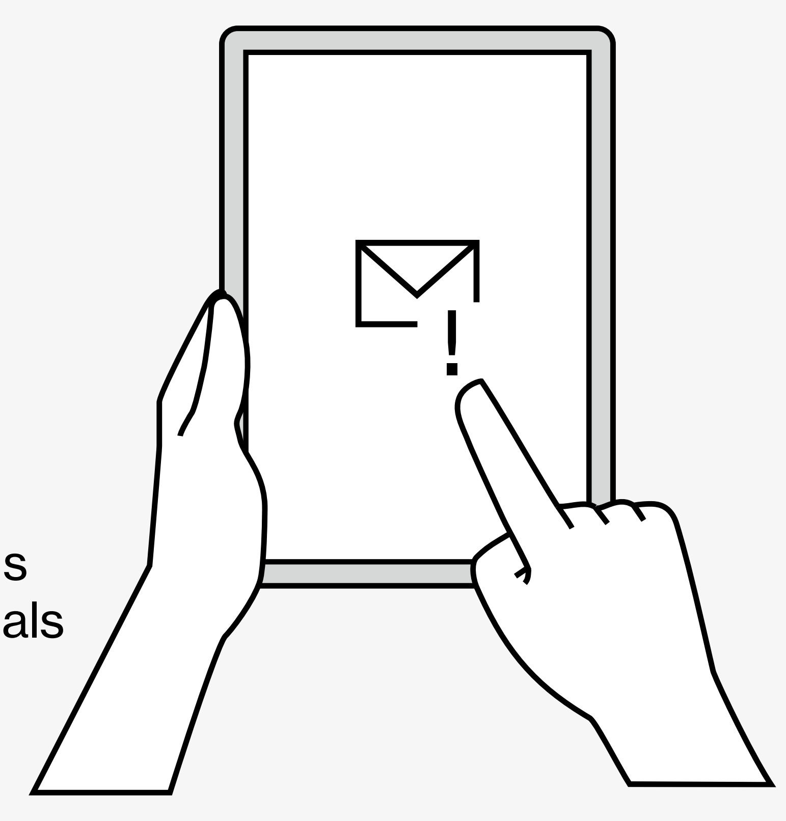


68 % der Angriffe wurden durch Personen begünstigt, die entweder Social Engineering zum Opfer fielen oder unabsichtlich einen Fehler machten.

Die schnelle Phishing-Falle

< 60 Sek.

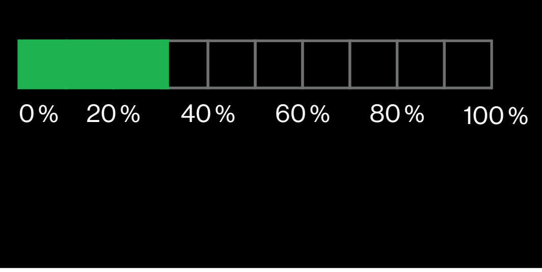
Die mittlere Zeit, in der Benutzer auf Phishing-E-Mails hereinfallen, beträgt weniger als 60 Sekunden.



Gestohlene Anmeldedaten sind weiterhin sehr begehrt.

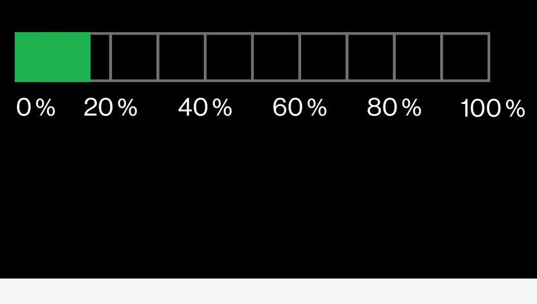
Bei 31 % aller Vorfälle in den vergangenen zehn Jahren spielten gestohlene Anmeldedaten eine Rolle.

31 %



Wählen Sie Ihre Drittanbieter sorgfältig aus.

15 %

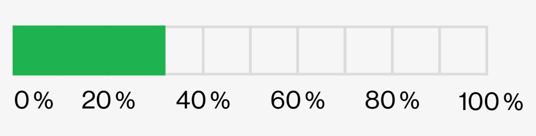


15 % der Angriffe verliefen über einen Dritten – zum Beispiel einen Hosting-Partner oder Datentreuhänder, in dessen Umgebung eingedrungen wurde, oder einen direkten oder indirekten Softwarezulieferer.

„Schöne Daten. Es wäre schade darum, wenn ihnen etwas zustoßen würde."

Bei 32 % der Sicherheitsverstöße 2023 wurde Ransomware oder eine andere Erpressungstechnik genutzt.

32 %



46.000 USD

Der mittlere Verlust aufgrund von finanziell motivierten Angriffen mit Ransomware oder einer anderen Erpressungsart betrug 46.000 USD.[1]

Sicherheitsverstöße schlagen teuer zu Buche.

50.000 USD

Der mittlere Verlust aufgrund von Business-E-Mail-Compromise-Angriffen 2022 und 2023 betrug etwa 50.000 USD.[1]

Die Bedrohungslandschaft ist noch komplexer und gefährlicher geworden.

Informieren Sie sich über aktuelle Trends und neue Angriffstechniken, um Ihre Infrastruktur effektiver zu schützen. Lesen Sie den kompletten Data Breach Investigations Report 2024 von Verizon (auf Englisch), die fundierte, vertrauenswürdige Informationsquelle zu Cybersicherheitsverletzungen.

Und kontaktieren Sie Ihren Ansprechpartner bei Verizon, um herauszufinden, wie unser erfahrenes Team Ihr Unternehmen beim Kampf gegen Cyberangriffe unterstützen kann.

Lesen Sie den Bericht unter verizon.com/dbir.

verizon business

[1] Basierend auf Daten des Internet Crime Complaint Center des FBI.