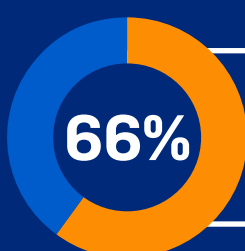


The State of Ransomware 2023

Die wichtigsten Ergebnisse aus der weltweiten Befragung von 3.000 IT-Experten.

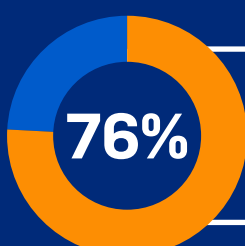


66% der Organisationen waren im letzten Jahr von Ransomware betroffen.

Häufigste Einfallstore:

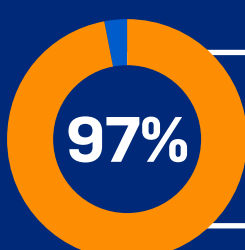
36% ausgenutzte Schwachstellen

29% kompromittierte Zugangsdaten



76% der Attacken hatten eine Verschlüsselung von Daten zur Folge.

Kriminelle entwendeten zusätzlich Daten in 30% der Angriffe, bei denen Daten verschlüsselt wurden.



97% der Organisationen, deren Daten verschlüsselt wurden, konnten diese wieder herstellen.

Die Nutzung von Backups fiel auf 70% im Vergleich zu 73% im Vorjahr. Die Prozentzahl der Organisationen, die Lösegeld bezahlten, blieb konstant bei 46%.



\$1.54Mio. betrug die durchschnittliche Lösegeldsumme. Fast doppelt so viel wie im Vorjahr mit \$812,380.

Lösegeld zahlende Unternehmen:

59% mit einer dedizierten Cyberversicherung

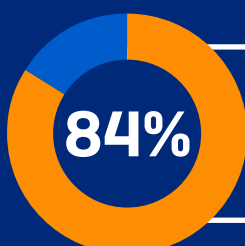
15% ohne Deckung durch eine Cyberversicherung



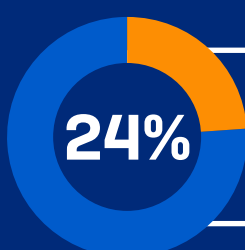
\$1.82Mio. betrugen die durchschnittlichen Kosten zur Wiederherstellung [exkl. der Lösegeldzahlung].

\$2.6Mio. bei Lösegeldzahlung mit Datenrückgabe

\$1.6Mio. bei Backup-Nutzung zur Datenwiederherstellung



84% der betroffenen Unternehmen hatten Geschäfts- bzw. Umsatzeinbußen [nur privater Sektor].



24% der betroffenen Unternehmen brauchten 1-6 Monate, um sich von der Ransomware-Attacke zu erholen.

Erholung innerhalb einer Woche:

45% beim Einsatz von Backups

39% bei Lösegeldzahlung

Der komplette Report ist verfügbar unter www.sophos.com/ransomware2023