SOPHOS

VCU IT-Systemhaus

Ransomware-Report 2024: Deutschland

Ergebnisse einer unabhängigen Befragung von 500 IT-Entscheidern aus deutschen Unternehmen und Organisationen mittlerer Größe.

Sophos-Whitepaper, April 2024

Über die Studie

Sophos hat eine unabhängige Befragung von 5.000 IT-/Cybersecurity-Entscheidern in Unternehmen und Organisationen mittlerer Größe (100–5.000 Mitarbeiter) aus 14 Ländern durchgeführt, darunter 500 in Deutschland. Die Befragung fand von Januar bis Februar 2024 statt. Die Umfrageteilnehmer wurden gebeten, sich bei der Beantwortung der Fragen auf ihre Erfahrungen in den letzten 12 Monaten zu beziehen. Alle Finanzdaten sind in US-Dollar angegeben.

Wichtigste Erkenntnisse

- **58 % der deutschen Unternehmen/Organisationen wurden im letzten Jahr Opfer von Ransomware.** Dieser Wert entspricht dem Vorjahr. Verglichen mit 67 % im Jahr 2022 ist dennoch ein erfreulicher Rückgang festzustellen. Weltweit gaben 59 % der Befragten an, dass ihr Unternehmen/ihre Organisation in den letzten zwölf Monaten von einem Ransomware-Angriff betroffen war.
- **Im Durchschnitt waren 54 % der Computer von dem Angriff betroffen**. Dieser Wert liegt über dem weltweiten Durchschnitt von 49 %.
- **Ausgenutzte Schwachstellen waren die häufigste Angriffsursache** bei Unternehmen/Organisationen in Deutschland. Sie wurden bei 34 % der Fälle zum Einfallstor. Kompromittierte Zugangsdaten waren die zweithäufigste Angriffsmethode und kamen bei 28 % der Angriffe zum Einsatz.
- **79 % der Angriffe führten zu einer Verschlüsselung von Daten**. Dieser Wert liegt über dem weltweiten Durchschnitt von 70 % und den 71 %, die von den Befragten aus Deutschland im letzten Jahr gemeldet wurden.
- **30 % der Angriffe, bei denen Daten verschlüsselt wurden, gingen zudem mit Datendiebstahl einher.** Dieser Wert liegt leicht unter dem weltweiten Durchschnitt von 32 %, entspricht aber dem Wert vom Vorjahr, in dem von deutschen Befragten in unserer Studie ebenfalls ein Anteil von 30 % gemeldet wurde.
- **Bei 93 % der deutschen Ransomware-Angriffe versuchten Cyberkriminelle, die Backups des Unternehmens/der Organisation zu kompromittieren.** Dieser Wert liegt knapp unter dem weltweiten Durchschnitt von 94 %.
- **63 % der Versuche, Backups zu kompromittieren, waren erfolgreich –** leicht über dem weltweiten Durchschnitt von 57 %.
- **98 % der deutschen Unternehmen/Organisationen, deren Daten verschlüsselt wurden, erhielten Daten zurück, was** dem weltweiten Durchschnitt von 98 % entspricht, aber leicht unter dem Wert von 99 % im Vorjahr liegt.
- **Backups bleiben die am häufigsten verwendete Methode zur Wiederherstellung von Daten –** 75 % der deutschen Befragten, deren Daten verschlüsselt wurden, griffen auf diese Strategie zurück**.** Dieser Wert ist ein Rückgang ggü. den 78 %, die in unserer Umfrage von 2023 angaben, Backups zu verwenden.
- **42 % der in Deutschland von Datenverschlüsselung Betroffenen zahlten das Lösegeld,** verglichen mit 44 % im Vorjahr und weniger als der weltweite Durchschnitt von 56 % im Jahr 2024.
- **46 % der deutschen Unternehmen/Organisationen, deren Daten verschlüsselt wurden, nutzten mehrere Wiederherstellungsmethoden**, um Daten zurückzubekommen, knapp unter dem weltweiten Durchschnitt von 47 %.
- 161 Befragte aus Deutschland, deren Daten verschlüsselt wurden, nannten die ursprüngliche Lösegeldforderung:
  - **Durchschnittliche Lösegeldforderung in Deutschland: 5.511.741 US$**; weltweit durchschnittl. 4.321.880 US$
  - Mittlere Lösegeldforderung in Deutschland: 4.400.000 US$; weltweit durchschnittl. 2 Mio. US$
  - 82 % der Forderungen betrugen mindestens 1 Mio. US$
- 96 Befragte aus Deutschland, deren Unternehmen/Organisation von Ransomware betroffen war und das Lösegeld gezahlt hatte, nannten die Lösegeldsummen:
  - **Durchschnittliche Lösegeldzahlung in Deutschland: 7.066.051 US$**; weltweit durchschnittl. 3.960.917 US$
  - Mittlere Lösegeldzahlung in Deutschland: 5.505.500 US$; weltweit durchschnittl. 2 Mio. US$
- **Deutsche Unternehmen/Organisationen zahlten durchschnittlich 106 % der ursprünglichen Lösegeldforderung.** Im Vergleich dazu beglichen Unternehmen/Organisationen weltweit 94 % der ursprünglichen Forderung.

- **81 % der deutschen Lösegeldzahlungen wurden aus verschiedenen Quellen finanziert,** knapp unter dem weltweiten Durchschnitt von 82 %.
- **Cyber-Versicherungsanbieter beteiligten sich in 81 % der Vorfälle am Lösegeld,** zahlten aber nur in 1 % der Fälle die volle Lösegeldsumme.
- Ohne Berücksichtigung von Lösegeldzahlungen meldeten deutsche Unternehmen/Organisationen nach einem Ransomware-Angriff **durchschnittliche Wiederherstellungskosten in Höhe von 2,20 Mio. US$.** Ein leichter Rückgang ggü. den 2023 gemeldeten 2,23 Mio US$. Dazu gehören Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangene Geschäftschancen etc.
- **Deutsche Unternehmen/Organisationen benötigten mehr Zeit zur Wiederherstellung nach einem Angriff**. 24 % gelang es, die Angriffsfolgen in bis zu einer Woche beseitigen, verglichen mit 43 % im Jahr 2023. 34 % benötigten zwischen einem und sechs Monaten, ein deutlicher Anstieg gegenüber dem Wert von 30 % im Vorjahr.
- **98 % der deutschen Ransomware-Opfer meldeten den Angriff** den Strafverfolgungsbehörden und/oder einer offiziellen Regierungsstelle.
  - 56 % erhielten Handlungsempfehlungen zum Umgang mit dem Angriff
  - 51 % erhielten Hilfe bei der Analyse des Angriffs
  - 43 % erhielten Unterstützung bei der Wiederherstellung von Daten, die während des Angriffs verschlüsselt wurden
- **56 % der Personen, die den Angriff meldeten, fanden die Zusammenarbeit mit den Strafverfolgungsbehörden und/oder offiziellen Stellen einfach.** 28 % empfanden den Prozess als relativ schwierig, 15 % als sehr schwierig.

Empfehlungen

Ransomware bleibt eine der größten Bedrohungen für die Sicherheit sämtlicher deutscher Unternehmen/Organisationen. Während die Gesamtangriffsrate im Vergleich zum Vorjahr konstant blieb, waren die Auswirkungen der Angriffe schwerwiegender. Da Angreifer ihre Angriffsmethoden ständig verbessern und weiterentwickeln, muss die Cyberabwehr der Unternehmen und Organisationen damit Schritt halten.

Prävention. Der beste Ransomware-Angriff ist ein abgewehrter Angriff, bei dem die Angreifer sich keinen Zugang zu Ihrem Unternehmen verschaffen konnten.

Schutz. Ein starkes Sicherheitsfundament ist ein Muss. Endpoints (einschließlich Server) sind das Hauptziel von Ransomware-Akteuren. Stellen Sie daher sicher, dass diese umfassend geschützt sind, unter anderem mit speziellem Anti-Ransomware-Schutz, um bösartige Verschlüsselungen zu stoppen und rückgängig zu machen.

Detection and Response. Je eher Sie einen Angriff stoppen, desto besser. Wenn Sie Angreifer in Ihrer Umgebung erkennen und stoppen, bevor sie Ihre Backups kompromittieren oder Ihre Daten verschlüsseln, können Sie die Auswirkungen des Angriffs erheblich abmildern.

Planung und Vorbereitung. Mit einem Incident-Response-Plan, d. h. einem Plan für die Reaktion auf Vorfälle, mit dem Sie sich eingehend beschäftigen, reduzieren Sie erheblich die Auswirkungen eines schwerwiegenden Vorfalls.

Sie möchten mehr darüber erfahren, wie Sophos Sie bei der Optimierung Ihrer Ransomware-Abwehr unterstützen kann? Sprechen Sie mit einem unserer Ansprechpartner oder besuchen Sie unsere Website unter www.sophos.de

Erfahren Sie mehr über Ransomware und darüber, wie Sophos Sie und Ihr Unternehmen oder Ihre Organisation davor schützen kann.

VCU GmbH
Nohner Str. 10 66693 Mettlach
Tel: 06868/91090
E-mail: vcu@vcu.de | Web: www.vcu.de

Sophos bietet branchenführende Cybersecurity-Lösungen für Unternehmen jeder Größe und schützt Kunden in Echtzeit vor komplexen Bedrohungen wie Malware, Ransomware und Phishing. Bewährte Next-Gen-Funktionen mit der Power von Machine Learning und künstlicher Intelligenz sichern Unternehmensdaten effektiv.

2024-04-22 (WP-PS)

VCU IT-Systemhaus

SOPHOS