SOPHOS
Cybersecurity delivered.

Ransomware-Report 2022: Deutschland

Ergebnisse einer unabhängigen Befragung von 400 IT-Entscheidern in mittelständischen Unternehmen in Deutschland.

Sophos-Whitepaper. April 2022

Über die Studie

Sophos beauftragte das Marktforschungsunternehmen Vanson Bourne mit der Durchführung einer unabhängigen Befragung von 5.600 IT-Fachleuten in mittelständischen Unternehmen (100–5.000 Mitarbeiter) aus 31 Ländern, darunter 400 in Deutschland. Die Befragung fand im Januar und Februar 2022 statt. Die Umfrageteilnehmer wurden gebeten, sich bei der Beantwortung der Fragen auf ihre Erfahrungen innerhalb des vergangenen Jahres zu beziehen.

Wichtigste Erkenntnisse

- **67 % der Befragten in Deutschland gaben an, dass ihr Unternehmen im letzten Jahr von Ransomware betroffen war** – dies entspricht einem deutlichen Anstieg gegenüber 2020, als nur 46 % von einem Ransomware-Angriff berichteten. Zum Vergleich: Weltweit verzeichneten 66 % der Befragten 2021 einen Ransomware-Angriff.
- **61 % der Angriffe führten zu einer Verschlüsselung von Daten.** Dieser Wert liegt leicht unter dem weltweiten Durchschnitt von 65 % und entspricht einem deutlichen Anstieg gegenüber den 49 %, die von den deutschen Befragten 2020 gemeldet wurden.
- **99 % der betroffenen Unternehmen, deren Daten verschlüsselt wurden, bekamen einen Teil ihrer Daten zurück.** Dies stimmt mit den globalen Ergebnissen überein, bei denen ebenfalls 99 % angaben, zumindest einen Teil ihrer Daten zurückerhalten zu haben.
- **Backups waren die am häufigsten genutzte Methode zur Wiederherstellung von Daten – 71 %** der deutschen Befragten, deren Daten verschlüsselt wurden, griffen auf Backups zurück. **42 % zahlten das Lösegeld.** Diese Ergebnisse zeigen klar, dass die parallele Nutzung mehrerer Methoden zur Datenwiederherstellung mittlerweile die Norm ist. Zum Vergleich: Weltweit nutzten 73 % der Befragten Backups und 46 % zahlten Lösegeld, um ihre Daten wiederherzustellen.
- **Durchschnittlich erhielten deutsche Unternehmen nach der Zahlung von Lösegeld 64 % ihrer Daten zurück.** Weltweit lag dieser Anteil bei 61 %, ein leichter Rückgang gegenüber dem Wert von 2020 (65 %).
- 56 der deutschen Befragten nannten die genaue Lösegeldsumme, die ihr Unternehmen gezahlt hat. **Die durchschnittliche Zahlung betrug 273.453 US-Dollar**. 13 % zahlten weniger als 10.000 USD, 9 % zahlten 1 Mio. USD oder mehr. Weltweit betrug die durchschnittliche Lösegeldzahlung 812.360 USD, und der Anteil der Unternehmen, die 1 Mio. USD oder mehr bezahlten, stieg um fast das Dreifache (von 4 % im Jahr 2020 auf 11 % im Jahr 2021).
- **Der Folgekosten eines Ransomware-Angriffs betrugen für deutsche Unternehmen im Jahr 2021 durchschnittlich 1,73 Mio. US-Dollar.** Dies entspricht einem deutlichen Anstieg gegenüber 2020, als die durchschnittlichen Kosten noch 1,17 Mio. USD betrugen.
- **92 % der Befragten in Deutschland gaben an, dass sie durch den Ransomware-Angriff in ihrer Betriebsfähigkeit beeinträchtigt wurden.** Dieser Wert ist auf globaler Ebene ähnlich (90 %).
- **84 % gaben an, dass ihr Unternehmen durch den Ransomware-Angriff Geschäftseinbußen oder Umsatzverluste hinnehmen musste.** Auch dies entspricht ungefähr dem weltweiten Wert von 86 %.
- **Die deutschen Befragten gaben an, dass ihr Unternehmen durchschnittlich einen Monat brauchte, um sich von dem Angriff zu erholen.**
- **80 % der deutschen Unternehmen haben eine Cyberversicherung, die bei einem Ransomware-Angriff für den Schaden aufkommt.** Weltweit liegt dieser Wert bei 83 %.
- **90 % sagten, es sei im letzten Jahr schwieriger geworden, eine Cyberversicherung abzuschließen.** 47 % berichteten, dass sie jetzt ein höheres Maß an Cybersicherheit nachweisen müssten, um eine

Versicherung abschließen zu können. 42 % meinten, dass die Policen jetzt komplexer seien, 37 % gaben an, dass der Bearbeitungsprozess länger dauere. 24 % sagten, der Versicherungsschutz sei teurer geworden. Da die Preise bei den Cyberversicherungen erst im zweiten und dritten Quartal 2021 anfingen zu steigen, waren die Auswirkungen für viele Unternehmen zum Zeitpunkt der Umfrage vermutlich noch nicht spürbar.

- **96 % haben ihre Cyberabwehr im letzten Jahr überarbeitet, um ihren Versicherungsstatus zu verbessern**. Weltweit haben 97 % Änderungen an ihrer Cyberabwehr vorgenommen: 64 % haben neue Technologien/Dienstleistungen eingeführt, 56 % bieten mehr Aus- und Weiterbildungsmaßnahmen für ihre Mitarbeiter an und 52 % haben ihre Prozesse/Verhaltensweisen geändert.
- **Cyberversicherungen zahlten bei Ransomware-Schäden in Deutschland in 98 % der Fälle.** Von den Ransomware-Opfern mit einer Cyberversicherung gegen Ransomware gaben 74 % an, dass ihr Versicherer die Bereinigungskosten übernommen habe. Bei 41 % zahlte die Versicherung das Lösegeld und bei 28 % wurden sonstige Kosten übernommen.

Fazit

Ransomware-Angriffe sind eine wachsende Bedrohung für deutsche Unternehmen. Optimaler Cyberschutz ist daher für alle Unternehmen unerlässlich. Unsere fünf wichtigsten Tipps für Sie:

- Sorgen Sie an allen Stellen in Ihrer gesamten Umgebung für einen hochwertigen Schutz. Überprüfen Sie Ihre Sicherheitskontrollen und stellen Sie sicher, dass sie Ihren Anforderungen entsprechen.
- Gehen Sie proaktiv auf die Suche nach Bedrohungen, damit Sie Angreifer stoppen können, bevor sie ihren Angriff ausführen können – wenn Sie nicht über entsprechende Ressourcen verfügen, beauftragen Sie einen MDR-Spezialisten.
- Härten Sie Ihre Umgebung, indem Sie nach Sicherheitslücken suchen und diese schließen. Dazu gehören z. B. ungepatchte Geräte, ungeschützte Rechner und offene RDP-Ports. XDR ist für diesen Zweck optimal geeignet.
- Planen Sie im Vorfeld für den Ernstfall. Legen Sie fest, welche Maßnahmen Sie im Fall eines Cyberangriffs ergreifen, und spielen Sie alle Schritte im Vorfeld durch.
- Erstellen Sie Backups und üben Sie, damit Ihre Daten wiederherzustellen. Ihr Ziel ist es, den Betrieb schnell wieder aufzunehmen.

Weitere Informationen

Alle weltweiten Werte sowie nach Branchen aufgeschlüsselte Daten finden Sie im Ransomware-Report 2022.

Ausführliche Informationen zu einzelnen Ransomware-Gruppen finden Sie im Sophos Ransomware Threat Intelligence Center.

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

2022-04-07 (WP-NP)

SOPHOS