SOPHOS

The State of Ransomware in Germany 2023

Findings from an independent, vendor-agnostic survey of 300 IT professionals in mid-sized organizations in Germany.

A Sophos Whitepaper. May 2023

About the survey

Sophos commissioned an independent, vendor-agnostic survey of 3,000 IT/cybersecurity leaders in mid-sized organizations (100-5,000 employees) across 14 countries, including 300 respondents in Germany. The survey was conducted between January and March 2023, and respondents were asked to respond based on their experiences in the previous 12 months.

Key findings

- **58% of German organizations were hit by ransomware in the last year,** a welcome decrease from the 67% that reported an attack in our 2022 survey. By comparison, globally, 66% of respondents said their organization had experienced a ransomware attack in the last twelve months.
- **Compromised credentials were the most common root cause of attack** for German organizations, used in 36% of incidents. Exploited vulnerabilities were the second most frequent attack vector, used in 24% of attacks.
- **71% of attacks resulted in data being encrypted.** This is slightly lower than the global average of 76%, but a significant increase from the 61% reported by German respondents in last year's survey.
- **Data was also stolen in 30% of attacks where data was encrypted**, in line with the global average of 30%.
- **95% of German organizations whose data was encrypted got data back,** slightly below the global average of 97%.
- **Backups remain the most common method used for restoring data,** with 78% of German respondents whose data was encrypted using this approach. This is slightly higher than the 71% that used backups in our 2022 survey.
- **44% of those that had data encrypted in Germany paid the ransom,** slightly up from last year's rate of 42%. As in our 2022 survey, German respondents reported a slightly below average propensity to pay the ransom (global average 2023: 47%, 2022: 46%)
- **27% of German organizations that had data encrypted used multiple recovery methods** in parallel.
- 11 respondents from Germany whose organization paid the ransom shared the exact amount, with both the mean and median **ransom payments coming in considerably lower than the global average:**
  - Mean ransom payment: Germany $1,231,428; global average $1,542,330
  - Median ransom payment: Germany $74,900; global average $400,000

  82% paid up to $1 million and 18% paid $1 million or more.
- Excluding any ransom payments, **the average (mean) bill incurred by German organizations to recover from a ransomware attack was reported at $2.23 million,** including costs of downtime, people time, device cost, network cost, lost opportunity, et cetera. This is above the global average cost of $1.82 million.
- **87% of private sector German organizations hit by ransomware said the attack caused them to lose business/revenue,** higher than the global average of 84%.
- **43% of German organizations took up to a week to recover from the attack.** 27% took up to a month while 30% took between one and six months.

- **90% of German organizations say they have some form of cyber insurance** with 43% having a standalone cyber policy and 47% having cyber as part of a wider business policy. By comparison, globally, 91% have cyber coverage with 47% having a standalone policy and 43% a wider business policy that covers cyber.
- **96% of German respondents** whose organization had purchased cyber insurance in the last year **said the quality of their defenses had a direct impact on their insurance position.**
  - 75% said it impacted the cost of their coverage (the premium)
  - 62% said it impacted their ability to get coverage
  - 25% said it impacted the terms of their policy, for example the total amount of coverage or sub-limits

Conclusion

Ransomware continues to be a major threat facing German organizations. With the growth of the ransomware-as-a-service business model, we do not anticipate a drop in attacks in the coming year. In this light, organizations should focus on:

- Further strengthening their defensive shields with:
  - Security tools that defend against the most common attack vectors, including endpoint protection with strong anti-exploit capabilities to prevent exploitation of vulnerabilities, and zero trust network access (ZTNA) to thwart the abuse of compromised credentials
  - Adaptive technologies that respond automatically to attacks, disrupting adversaries and buying defenders time to respond
  - 24/7 threat detection, investigation, and response, whether delivered in-house or in partnership
- Optimizing attack preparation, including making regular backups, practicing recovering data from backups, and maintaining an up-to-date incident response plan
- Maintaining good security hygiene, including timely patching and regularly reviewing security tool configurations

Further information

Read The State of Ransomware 2023 report for the full global findings and data by sector.

Learn more about ransomware and how Sophos can help you defend your organization.

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

© Copyright 2023. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2023-05-05 (WP-PC)

SOPHOS