SOPHOS

The State of Ransomware in South Africa 2023

Findings from an independent, vendor-agnostic survey of 200 IT professionals in mid-sized organizations in South Africa.

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 200 respondents in South Africa. 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

- **78% of South African organizations were hit by ransomware in the last year**, a considerable increase from the 51% 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.
- **Exploited vulnerabilities were the most common root cause of attack** for South African organizations, used in 49% of incidents. Compromised credentials were the second most frequent attack vector, used in 24% of attacks.
- **89% of attacks resulted in data being encrypted**. This is higher than the global average of 76%, and a considerable increase from the 45% reported by South African respondents in last year's survey.
- **Data was also stolen in 35% of attacks where data was encrypted**, higher than the global average of 30%.
- **100% of South African organizations whose data was encrypted got data back**, slightly above the global average of 97%.
- **Backups remain the most common method used for restoring data**, with 76% of South African respondents whose data was encrypted using this approach. This is in line with the 80% that used backups in our 2022 survey.
- **45% of those that had data encrypted in South Africa paid the ransom**, slightly down from both last year's rate of 49% and the 2023 global average of 47%.
- **24% of South African organizations that had data encrypted used multiple recovery methods** in parallel.
- Two respondents from the South African whose organization paid the ransom shared the exact amount. One of these respondents reported **paying $5 million or more**.
- Excluding any ransom payments, **the average (mean) bill incurred by South African organizations to recover from a ransomware attack was reported at $0.75 million**, including costs of downtime, people time, device cost, network cost, lost opportunity, et cetera. This is considerably less than the global average cost of $1.82 million.
- **82% of private sector South African organizations hit by ransomware said the attack caused them to lose business/revenue**, slightly lower than the global average of 84%.
- **53% of South African organizations took up to a week to recover from the attack**. 29% took up to a month while 19% took between one and six months.
- **98% of South African organizations say they have some form of cyber insurance** with 47% having a standalone cyber policy and 51% 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.

- **98% of South African 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**.
  - 66% said it impacted their ability to get coverage
  - 61% said it impacted the cost of their coverage (the premium)
  - 19% 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 South African 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 with a specialist Managed Detection and Response (MDR) service provider
- 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.

2023-05-09 (WP-MP)

SOPHOS