SOPHOS

THE STATE OF RANSOMWARE IN GERMANY 2026

Findings from an independent, vendor-agnostic survey of 139 organizations in Germany that were hit by ransomware in the last year.

A SOPHOS WHITEPAPER - JULY 2026

About the report

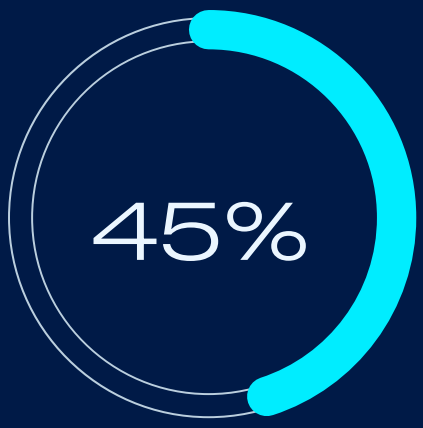
Now in its seventh year, the State of Ransomware report is based on the findings from an independent, vendor-agnostic survey commissioned by Sophos. This year's global report is based on the experiences of 2,158 IT/cybersecurity leaders working in organizations that were hit by ransomware in the last year, including 139 from Germany.

The survey was conducted between January and March 2026. All respondents work in organizations with between 100 and 5,000 employees and were asked to answer based on their experiences in the previous 12 months. All financial data points are in U.S. dollars. Outlier ransoms of $40 million or more were removed from this data.

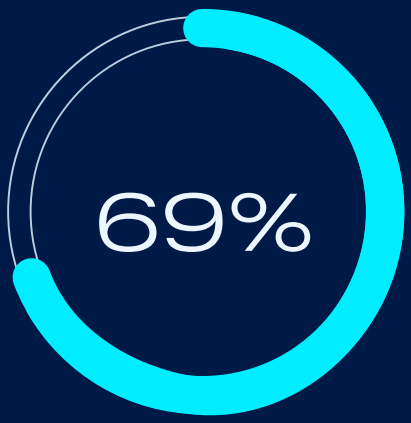
Survey of

139

IT/cybersecurity leaders in Germany working in organizations that were hit by ransomware in the last year.



Percentage of attacks that resulted in data being encrypted.



Confirmed that this past year's ransomware incident was the same event as their most significant identity attack.

Average cost to recover from a ransomware attack.

Why German organizations fall victim to ransomware

- **Phishing was the most common technical root cause of attack,** used in 30% of attacks, followed by compromised credentials (24%) and malicious email (20%). Exploited vulnerabilities dropped sharply, falling to 17% from 42% in the 2025 report.
- **(NEW) 69% confirmed that this past year's ransomware incident was the same event as their most significant identity attack.**
- **(NEW) Exposed applications and systems were the most common attack entry point (32%)** for non-email, non-phishing root causes, followed by user devices (31%) and firewalls (25%).
- **Poor quality protection (40%) was the most common operational root cause,** followed by an unknown security gap and a lack of expertise, which were tied for second at 39% each.

What happens to the data

- **45% of attacks resulted in data being encrypted.** This is below the global average of 56% and a drop from the 51% reported by German respondents in the 2025 report.
- **Data was also stolen in 24% of attacks where data was encrypted,** in line with the 24% reported in 2025.
- **97% of German organizations that had data encrypted were able to get it back,** in line with the global average.
- **45% of German organizations paid the ransom and got data back,** a considerable drop from the 63% reported in last year's report.
- **61% of German organizations used backups to recover encrypted data,** a slight increase from the 59% reported in the 2025 report.

Ransom demands

- **The median German ransom demand was $400,000,** a 33% drop from the $600,000 reported in the 2025 report.
- **45% of ransom demands were for $1 million or more,** down from the 49% reported in the 2025 report.

Median German ransom demand.

Business impact of ransomware

- **Excluding any ransom payments, the average (mean) cost incurred by German organizations to recover from a ransomware attack in this year's report came in at $1.42 million,** a slight decrease from the $1.56 million mean reported in the 2025 report. This includes the costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **60% of German organizations recovered from a ransomware attack in up to a week,** a slight drop from the 64% reported in the 2025 report. 12% took between one and six months to recover, a small increase from the 9% in the 2025 report.

Human impact of ransomware on IT/cybersecurity teams in organizations where data was encrypted

45% report increased anxiety or stress about future attacks.

45% report increased feelings of guilt that the attack was not stopped.

44% report a change of team priorities/focus.

40% report increased pressure from senior leaders.

27% report that the team's leadership has been replaced.

Recommendations

Strengthen identity security as a ransomware defense. Nearly two-thirds of German ransomware victims confirmed their ransomware incident was the same event as their most significant identity attack. Organizations should prioritize identity threat detection and response (ITDR), enforce multi-factor authentication across all access points, and regularly audit both human and non-human identity credentials.

Strengthen endpoint protection for AI frontier models. Frontier AI is accelerating vulnerability discovery and exploitability. Having strong endpoint defenses that automatically block exploit-based attacks is essential.

Prioritize email security. With phishing and malicious email accounting for nearly half of ransomware root causes in Germany, organizations should deploy advanced email filtering, implement DMARC/DKIM/SPF protocols, and invest in regular phishing awareness training.

Invest in backup and recovery infrastructure. Organizations that maintained robust backup systems recovered encrypted data at nearly record rates in the past year. Backups should be tested regularly, stored offline or in immutable formats, and integrated into a documented incident response plan that can be executed under pressure.

SOPHOS

To explore how Sophos can help you optimize your ransomware defenses, speak to an advisor or visit **sophos.com/ransomware2026**

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.

2026-08-03 DE-WP (TA) CRE-6007