

THE STATE OF RANSOMWARE IN GERMANY 2025

Findings from an independent, vendor-agnostic survey of 300 organizations in Germany that were hit by ransomware in the last year.

About the report

This report is based on the findings of an independent, vendor-agnostic survey of 3,400 IT/cybersecurity leaders working in organizations that were hit by ransomware in the last year, including 300 from Germany.

The survey was commissioned by Sophos and conducted by a third-party specialist between January and March 2025.

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.

The report includes comparisons with the findings from our 2024 survey. All financial data points are in U.S. dollars.

Survey of
300

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



51%

Percentage of attacks
that resulted in data
being encrypted.



\$412K

Median German
ransom payment
in the last year.



\$1.56M

Average cost to
recover from a
ransomware attack.

Why German organizations fall victim to ransomware

- ▶ **Exploited vulnerabilities were the most common technical root cause of attack**, used in 42% of attacks. They are followed by compromised credentials, which were the start of 20% of attacks. Malicious emails were used in 19% of attacks.
- ▶ **A lack of people / capacity was the most common operational root cause**, cited by 47% of German respondents. 45% said both known and unknown security gaps played a factor in their organization falling victim to ransomware.

What happens to the data

- ▶ **51% of attacks resulted in data being encrypted**. This is in line with the global average of 50% but a significant drop from the 79% reported by German respondents in 2024.
- ▶ **Data was also stolen in 24% of attacks where data was encrypted**, a drop from the 30% reported last year.
- ▶ **95% of German organizations that had data encrypted were able to get it back**, just below the global average.
- ▶ **63% of German organizations paid the ransom and got data back**, a considerable increase from the 42% reported last year.
- ▶ **59% of German organizations used backups to recover encrypted data**, a notable drop from the 75% reported last year.

Ransoms: Demands and payments

- ▶ **The median German ransom demand in the last year was \$600,000**, which is an 86% drop from the \$4.4 million reported in our 2024 survey.
- ▶ **49% of ransom demands were for \$1 million or more**, down from 62% in 2024.
- ▶ **The median German ransom payment in the last year was \$411,600**, a 93% drop from the \$5.5 million reported last year.
- ▶ **German organizations typically paid 86% of the ransom demand**, in line with the global average of 85%.
 - 47% **paid LESS THAN** the initial ransom demand (global average: 53%)
 - 32% **paid THE SAME** as the initial ransom demand (global average: 29%)
 - 20% **paid MORE THAN** the initial ransom demand (global average: 18%)

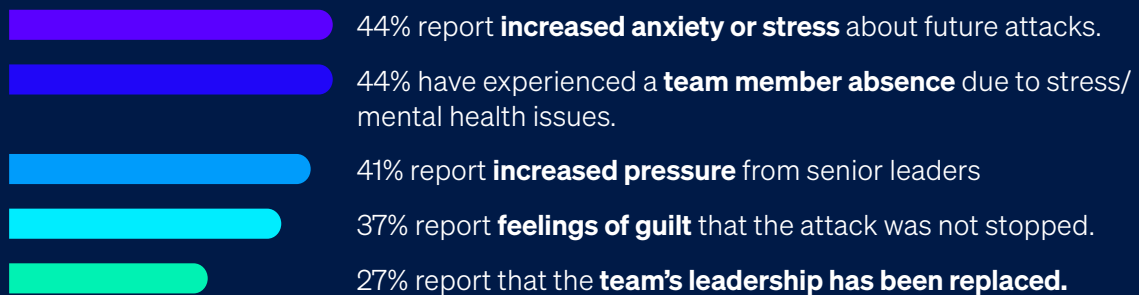


Median German ransom demand in the last year.

Business impact of ransomware

- ▶ Excluding any ransom payments, **the average (mean) bill incurred by German organizations to recover from a ransomware attack in the last year came in at \$1.56 million**, a drop from the \$2.2 million reported by German respondents in 2024. This includes costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- ▶ **German organizations are getting faster at recovering from a ransomware attack**, with 64% fully recovered in up to a week, a significant increase from the 24% reported last year. Just 9% took between one and six months to recover, a notable drop from last year's 34%.

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



Recommendations

Ransomware remains a major threat to German organizations. As adversaries continue to iterate and evolve their attacks, it's essential that defenders and their cyber defenses keep pace. The learnings from this report indicate key areas for focus in 2025 and beyond.

- ▶ **Prevention.** The best ransomware attack is the one that didn't happen because adversaries couldn't get into your organization. Look to reduce both the technical root causes of attack and the operational ones highlighted in this report.
- ▶ **Protection.** Strong foundational security is a must. Endpoints (including servers) are the primary destination for ransomware actors, so ensure that they are well defended, including dedicated anti-ransomware protection to stop and roll back malicious encryption.
- ▶ **Detection and response.** The sooner you stop an attack, the better your outcomes. Around-the-clock threat detection and response is now an essential layer of defense. If you lack the resources or skills to deliver this in house, look to work with a trusted managed detection and response (MDR) provider.
- ▶ **Planning and preparation.** Having an incident response plan that you are well versed in deploying will greatly improve your outcomes if the worst happens and you experience a major attack. Be sure to take good backups and regularly practice recovering from them.



To explore how Sophos can help you optimize your ransomware defenses, speak to an adviser or visit

sophos.com/ransomware2025

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.