Almost 60% of Businesses are 'Very' to 'Extremely' Concerned about Ransomware Attacks - Hornetsecurity Ransomware Survey

More than half of leadership teams are 'actively involved' in decision-making on preventing attacks. 1 in 5 respondents said their company was attacked in 2023.

One in five respondents said their company suffered an attack in 2023

NUREMBURG, GERMANY, October 10, 2023 /EINPresswire.com/ -- Nearly 60% of companies are 'very' to 'extremely' concerned about ransomware attacks, according to latest research from leading cybersecurity provider Hornetsecurity. The company released the survey results at IT-SA 2023, Europe's largest IT security trade show, where it is exhibiting.

In its annual Ransomware Survey, Hornetsecurity revealed that more than nine in ten (92.5%) businesses are aware of ransomware's potential for negative impact, but just 54% of respondents said their leadership is 'actively involved in conversations and decision-making' around preventing such attacks. Four in ten (39.7%) said they were happy to 'leave it to IT to deal with the issue'.

> Organizations cannot afford to become victims –ongoing security awareness training and multi-layered ransomware protection is critical to ensure there are no insurmountable losses."
>
> *Daniel Hofmann, Hornetsecurity CEO*

Commenting on the findings, Hornetsecurity CEO Daniel Hofmann, said: "Our annual Ransomware Survey is a timely reminder that ransomware protection is key to ongoing success. Organizations cannot afford to become victims –ongoing security awareness training and multi-layered ransomware protection is critical to ensure there are no insurmountable losses."

Ransomware protection is a necessity

Reassuringly, 93.2% of respondents rank ransomware

protection as ‘very’ to ‘extremely’ important in terms of IT priorities for their organization, and 87.8% of respondents confirmed they have a disaster recovery plan in place for a ransomware attack.

However, that leaves more than one in eight organizations (12.2%) without a disaster recovery plan. Of those companies, more than half cited a ‘lack of resources or time’ as the primary reason. Additionally, one-third of respondents said a disaster recovery plan is ‘not considered a priority by management’.

Comparing Ransomware Survey results in 2021-2023
This survey has been conducted annually over the past three years and has included asking respondents if their organization has fallen victim to a ransomware attack.

Since 2021, Hornetsecurity has found relatively small changes in the percentage of respondents saying their organizations have fallen victim to a ransomware attack: 21.1% in 2021, 23.9% in 2022, but a new low of 19.7% in 2023.

Additionally, companies that reported paying a ransom are down from 9.1% in 2021 to 6.9% in 2023.

Some of the data in this survey show positive results, with a majority of respondents reporting they understand the importance of protection, and a drop in ransomware attack victims in 2023, showing companies are becoming more vigilant in their data protection.

Ransomware attacks continue to evolve, though, so organizations must maintain this vigilance. In 2023, 81% of respondents reported they are receiving end-user training in comparison to 2021, when only 71.2% reported they had received training.

“Although organizations have reported fewer ransomware attacks in 2023, the threats haven’t necessarily decreased,“ Hofmann said. “Cybersecurity awareness among all users remains a crucial element to further decrease the risk of falling for these threats, especially as attacks become more sophisticated with new technologies.”

Security tools to combat ransomware attacks
The survey also revealed the most used tools to combat potential threats:
- 87.8% used to end-point detection software with anti-ransomware capabilities
- 84.4% cited ‘email filtration and threat analysis’
- 22.4% mentioned ‘AI-enabled security solutions’ as a tool they are now using to combat ransomware within their organization.

The most common primary security feature to protect backups from ransomware is:
- Immutable storage (40.6% of respondents)
- Tight control of user and application permissions (38.3%)

 Air-gapped storage (27.8%).

Given the unpredictable nature of ransomware attacks, 76.2% of respondents said their business has changed the way it backs up its data. The 73.6% of respondents who have a recovery plan in place for their Microsoft 365 data are ‘very’ to ‘extremely’ confident in their chosen solution, while 55.1% of respondents are ‘very’ to ‘extremely’ confident that their data backups would be safe from a ransomware attack today.

About the survey
Hornetsecurity’s Annual Ransomware Survey 2023 was answered by more than 150 business decision-makers (including IT pros) across small to large enterprises. This year's annual survey had 46.9% of respondents based in Europe, 30.6% in North America, with the other 21.5% from Asia, Australia, Africa, the Middle East and South America.

Find out more about Hornetsecurity’s latest ransomware survey.

About Hornetsecurity
Hornetsecurity is a leading global provider of next-generation cloud-based security, compliance, backup, and security awareness solutions that help companies and organizations of all sizes around the world. Its flagship product, 365 Total Protection, is the most comprehensive cloud security solution for Microsoft 365 on the market. Driven by innovation and cybersecurity excellence, Hornetsecurity is building a safer digital future and sustainable security cultures with its award-winning portfolio. Hornetsecurity operates in more than 30 countries through its international distribution network of 8,000+ channel partners and MSPs. Its premium services are used by more than 50,000 customers.

Media enquiries
Please contact us at press@hornetsecurity.com.

Angelica Micallef Trigona
Hornetsecurity
+356 2032 3461
email us here