# 1 in 5 companies has suffered a ransomware attack, survey finds

*The study on ransomware, conducted by cybersecurity experts at Hornetsecurity, also found that almost 1 in 10 ransomware victims paid the ransom.*

The study on ransomware, conducted by cybersecurity experts at Hornetsecurity, also found that almost 1 in 10 ransomware victims paid the ransom.

LONDON, UNITED KINGDOM, October 7, 2021 /EINPresswire.com/ -- A recent survey of 820+ businesses found that 21% of respondents had been the victim of a ransomware attack to date. Ransomware is one of the most common and effective forms of cyber threat, whereby attackers encrypt an organization's data, rendering it unusable until a ransom is paid.

Over 9% of surveyed ransomware victims paid the ransom

Of the 21% of companies that reported a ransomware attack, 9.2% recovered the data by paying the demanded ransom. The remaining respondents recovered the ransomed data through backups, yet some still reported losing data in the process.
According to the results, companies with 201-500 employees reported the highest incidence of ransomware attacks (25.3%), while those employing 1-50 had the lowest (18.7%). In geographical terms, 19.6% of North American companies reported attacks, while those based in Europe reported 21.2%.

Over 15% of companies do not protect backups from ransomware

15.2% of all survey respondents indicated that their company does not protect their backups from ransomware. Moreover, the survey also found that 17.2% of reported ransomware attacks targeted backup storage. These results reveal a cause for concern:  that standard on-site backups do not offer 100% protection against ransomware attacks. Indeed, backups must be protected against ransomware attacks through methods such as air-gapped, offsite storage or immutable storage - two commonly reported protection methods in this survey.

15.9% of respondents also reported having no disaster recovery plan in place, meaning they are typically unprepared and unequipped to deal with an attack.

28.7% of companies do not provide training to end-users on how to recognize and flag potential ransomware attacks

End-users represent one of the most effective methods-of-entry for ransomware attackers. Through social engineering techniques such as email phishing, end-users are manipulated into providing opportunities for malicious software to be introduced into company systems. According to this survey, more than 1 out of every 4 organizations (28.7%) do not provide training to end-users on how to recognize and handle potential ransomware threats.

Most common forms of backup and ransomware protection and prevention

71.3% of companies changed the way they back up their data in response to the threat of ransomware. The two most common forms of prevention observed in the survey are end-point detection software with anti-ransomware capabilities (75.6%), and email filtration and threat analysis (76.1%). Air-gapped, offsite storage is reported to be used 47.8% of the time - a low percentage when considering its effectiveness at enabling extraordinary data recovery.
To read more about the survey, along with a more in-depth analysis, click here.

About Hornetsecurity Group

Hornetsecurity is the leading security and backup solution provider for Microsoft 365. Its flagship product is the most extensive cloud security solution for Microsoft 365 on the market, providing robust, comprehensive, award-winning protection: Spam and virus filtering, protection against phishing and ransomware, legally compliant archiving and encryption, advanced threat protection, email continuity, signatures and disclaimers. It’s an all-in-one security package that even includes backup and recovery for all data in Microsoft 365 and users’ endpoints.

Media enquiries

Please contact us on marketing@hornetsecurity.com.

Angelica Micallef Trigona
Hornetsecurity
+356 2032 3461
marketing@hornetsecurity.com
Visit us on social media:
Facebook
Twitter
LinkedIn