HORNETSECURITY

INFO
SHEET

RANSOMWARE

HOW COMPANIES CAN EFFECTIVELY PROTECT THEMSELVES

> Ransomware is regarded as the most important cyber threat for organizations worldwide (source: World Economic Forum, 2025). Criminals increasingly adopt highly developed, automated attack chains that are becoming more sophisticated through the use of generative AI technologies. Particularly insidious: many attacks begin with seemingly harmless emails – and end with the encryption of entire systems. A recent survey by Hornetsecurity reveals that one in three companies experienced data loss due to ransomware in 2024.

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software that encrypts computers or files and blocks access to them until a ransom is paid. It is usually installed without being noticed and then makes direct contact with the victim. Ransomware is particularly dangerous because it can spread across networks and cripple entire organizations.

COMMON ATTACK VECTORS

Phishing attacks: Often, a single click on a malicious link or a reply to a manipulated email is enough to trigger an attack.

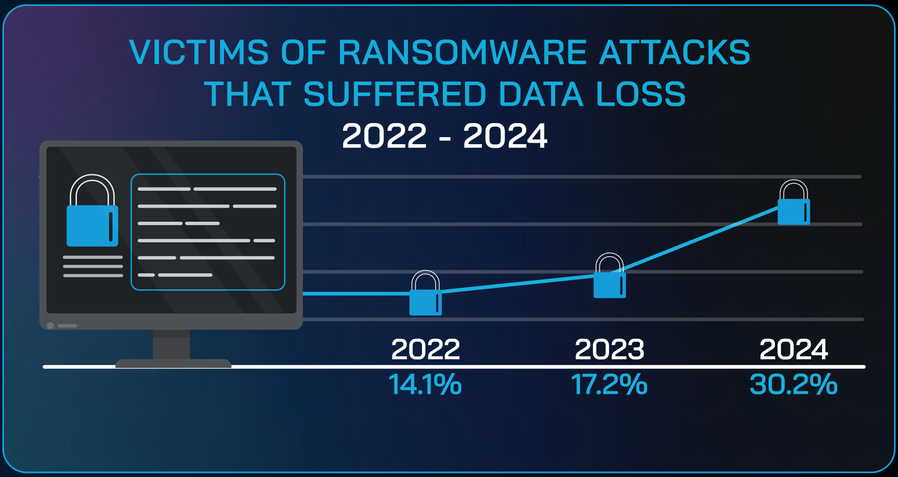
Emails & attachments: Ransomware is frequently spread via infected Office documents, ZIP files, or PDFs. Emails with personalized content are particularly difficult to detect and can bypass conventional filters.

Weak login credentials: Easy-to-guess passwords or missing multi-factor authentication (MFA) make it easier for attackers to gain system access.

Unpatched systems: Attackers exploit known vulnerabilities in software and systems. Hence, incomplete patching is a prime target for ransomware.

Social engineering tactics: Employees are deliberately manipulated, for example through phone calls or targeted support requests. Attackers often rely on stress, authority, or urgency to provoke impulsive actions.

HORNETSECURITY



VICTIMS OF RANSOMWARE ATTACKS THAT SUFFERED DATA LOSS
2022 - 2024

PROTECTION STRATEGIES AGAINST RANSOMWARE:

RELIABLY BLOCK MALICIOUS EMAILS	SPAM & MALWARE PROTECTION	Phishing emails remain one of the most common entry points for ransomware. Security solutions like Spam and Malware Protection block harmful attachments or infected links before any damage can occur.
DETECT MODERN THREATS EARLY ON	ADVANCED THREAT PROTECTION	Ransomware is becoming increasingly sophisticated. Protection based on self-learning AI can identify and stop hidden or new threats – use solutions such as Advanced Threat Protection.
KEEP AN EYE ON CRITICAL VULNERABILITIES		Attackers often exploit known security flaws in software or outdated systems to deploy ransomware. Keep your systems continuously updated, ideally with centralized patch management, and use multi-factor authentication wherever possible.
ACTIVELY INVOLVE EMPLOYEES	SECURITY AWARENESS	Even the best technology is powerless if human behavior becomes the weak point. Raise awareness among your teams through regular training and simulated phishing campaigns using Security Awareness Service – and foster a sustainable security culture in your organization.
QUICKLY RESTORE DATA IN CASE OF AN EMERGENCY	VM BACKUP 365 TOTAL BACKUP	Despite all prevention efforts, protection can never be 100% guaranteed. That's why protecting your data is crucial. With VM Backup V9 and 365 Total Backup, you can store your backups securely within Hornetsecurity's infrastructure – keeping your data safe from ransomware attacks.