Acronis

WHITE PAPER

A 12-step ransomware response plan for business

How to defend against and recover from the world's most urgent cyberthreat

In a few short years, ransomware has emerged as the malware tool of choice for cybercriminals to enrich themselves by threatening businesses with data loss and downtime. That surge has ballooned the average cost of a data breach to a projected $5 million per incident in 2023. The frequency of attacks is growing at an alarming rate as cybercriminals scale up their malware development and distribution operations, with nine million new malware samples appearing in the wild every month.

Meanwhile, cybercriminals are continually developing new tactics and exploiting new technologies like artificial intelligence (AI) to improve attack effectiveness. For instance, encryption of a target's critical data in a ransomware attack is no longer the sole method to extract ransoms. Most ransomware attackers now precede the encryption stage by first stealing sensitive data so they can threaten to leak it online if the target fails to pay the ransom. Attackers may also contact the target's customers and partners with the threat that their private data may also be leaked, adding pressure to comply with the extortion demand. Yet another tactic is the threat that failure to pay may result in a DDoS attack on the target's public servers.

Attackers are now also exploiting new AI tools like ChatGPT to improve the apparent authenticity and trustworthiness of phishing emails, to automatically scan applications for vulnerabilities, and to improve the orchestration of multistage attacks. AI-enabled improvements to attacks, new extortion tactics, and mushrooming attack frequency have led cyber insurers to drop coverage of businesses that cannot prove they have robust defenses in place, potentially eliminating a popular hedge against recovery costs.

Despite this grim outlook, businesses can take a range of concrete steps to significantly reduce the likelihood of a successful ransomware attack and to minimize the damage in downtime and lost data in the event an attack succeeds. Acronis recommends the adoption of the following 12-step plan to counter the ransomware threat, with tactics falling into three categories: active defense measures, new skills and processes for IT and employees, and reinforced attack mitigation and recovery programs.

Upgrade active defense measures

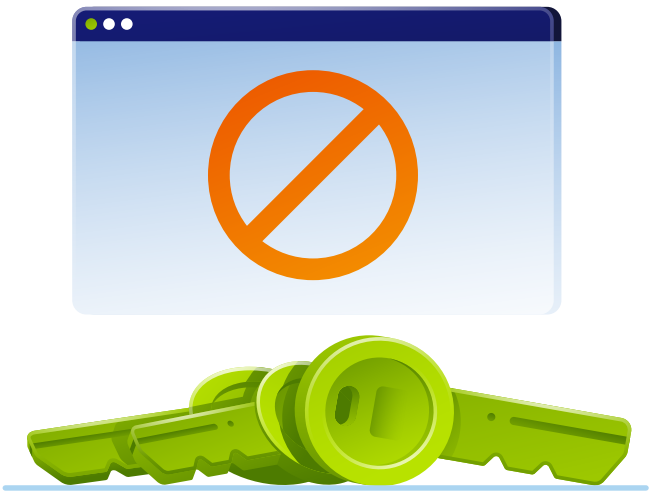
Step one **Deploy anti-malware measures that are capable of identifying ransomware by its behavior to complement legacy signature-based antivirus**. Machine learning and AI are crucial components here, as they enable the detection of patterns of malicious behavior as opposed to merely matching the signature of a malware instance against a database of known threats. Without this behavioral approach, no anti-malware measure can successfully identify the thousands of zero-day malware instances that are being generated by threat actors every day.

Step two **Update countermeasures like email security and URL filtering.** In 2022, 30.6% of all received emails were spam, while 1.6% contained malware or phishing links. Phishing was the vector used in 76% of all successful attacks in 2022, and roughly 8% of endpoints tried to access malicious URLs in 2022. Cybercriminals have gotten much better at obfuscating malicious links and attachments in emails, so one of the most effective acts of triage a business can perform is investing in up-to-date email security that will detect and filter out phishing emails before they hit the employee inbox.

Step three **Deploy tools that increase your visibility of IT resources and data flows.** A typical question from management to IT following a ransomware attack is, "How did an attacker exfiltrate a terabyte of our sensitive data without us knowing?" To help avoid this painful moment, monitor and log activity inside your infrastructure, including access to cloud services, and conduct ongoing log analysis. IT inventorying and data loss prevention (DLP) tools can also provide better visibility to where data is stored and how it is moving to detect data theft and lock down potential exposures. Consider deploying endpoint detection and response (EDR) technology, which uses real-time monitoring, behavioral analysis and machine learning to identify malware, intrusions and unauthorized access.

Step four **Eliminate external and internal network exposures.** Disable Microsoft Remote Desktop Protocol (RDP) except where it is necessary, and otherwise harden endpoints by disabling unused services. Use firewalls and intrusion prevention systems to limit inbound internet access. Consider limiting VPN access to specific geographic locations, and establishing a remote-work policy that limits or prohibits access to company resources from personal devices. To minimize potential threats from malicious or careless employees, segment your internal networks to thwart the propagation of ransomware from compromised systems to other endpoints and servers.

Step five **Manage passwords and access rights vigilantly.** Leaked or stolen credentials contributed to almost half of reported breaches in 2022. Ransomware attackers commonly exploit leaked passwords, passwords reused across multiple accounts, weak passwords, and single-factor authentication. Attackers often commandeer IT operations tools like Mimikatz to steal passwords stored in memory on servers. To combat these tactics, implement multifactor authentication, especially on systems with sensitive data. Always change administrative login credentials from their factory default settings. Change all passwords after a successful attack, as cybercriminals are known to re-attack a prior target using the same compromised credentials that enabled the first attack. Adopt the principle of least privilege for access rights. Tightly control access to systems with powerful administrative tools or sensitive data, excluding all but essential employees, and make privileges time-limited or one-time-only where possible.



Optimize skills and processes

Step six **Build a security awareness training program.** Phishing remains among the most effective techniques for getting malware inside a company's external defenses, so reducing the number of clicks on malicious attachments and links in emails (as well as in SMS, instant messaging and social media apps) can yield significant risk reductions. Train users to keep their antennae up for suspicious communications by routinely sending them fake phishing emails; offer refresher courses to those who fall for the ruse. Make sure every employee participates — especially executives, as they are favorite targets due to their elevated privileges and ability to authorize money transfers.

Step seven **Implement automated, programmatic vulnerability scanning and patch management.** The typical small to medium-sized business struggles to install software patches from its tech vendors in a timely fashion, leaving vulnerabilities unpatched for over 90 days on average. Cybercriminals are aware of these exposures and constantly probe for them. To close these gaps quickly and efficiently, apply automated tools to this tedious but critical IT operations chore.

Step eight **Reduce the number of agents on endpoints and consoles in your operations center.** The typical business has deployed its cybersecurity and data protection solutions in piecemeal fashion over time, resulting in a proliferation of remote agents on endpoints and management consoles at the IT operations desk. Multiple endpoint agents waste resources and often conflict with each other. Swiveling between consoles reduces IT operational efficiency and increases training costs. Consolidate agents wherever possible to eliminate gaps and conflicts and to improve endpoint performance. Combine management console functionality where possible to maximize the effectiveness and onboarding speed of IT personnel.

Step nine **Take advantage of security frameworks like NIST to regularly assess and update your defense and mitigation strategies for ransomware and other cyberthreats.** They offer proven best practices and guidance for prioritizing security remediations and continuously improving your technology, processes and people skills.

Reinforce attack mitigation and recovery

Step ten **Implement a robust data protection regimen.** Attackers always have first-mover advantage, and even the best defenses can fail to defeat new tactics and technology. Assume that an attack will succeed at some point, and strive to improve your data protection regimen as a last line of defense. Restoring data from a recent backup may enable the quick resumption of business operations — potentially without paying a ransom. However, note that attackers often attempt to locate and encrypt or delete backup archives, disable backup and security measures, and use your own operations and backup tools to steal data and spread the attack across your network. Thus, it is essential to keep multiple copies of backups, ideally encrypted, on different media and in different locations: off-site, offline, and in the cloud. Conduct regular live tests of your backup plan to validate the integrity of your archives and processes, and to ensure that you can execute restoral swiftly enough to meet your business's recovery time objectives. Finally, scan backups for malware and unpatched vulnerabilities and correct those issues before restoring systems and putting them back into production.

Step eleven **Consider implementing a disaster recovery program.** The process of cleanup and recovery after a ransomware attack, including the restoral of large amounts of data from backup, can postpone the resumption of normal business operations by days or weeks. The ability to immediately resume operations by switching over to replicated applications and data (either offsite or in the cloud) is a valuable hedge against this

kind of extended outage. The advent of disaster recovery as a service has made this contingency much more affordable and simple to manage — even for smaller businesses.

Step twelve **Build an incident response plan and regularly test and update it.** Have the names and numbers of essential internal and external contacts in hard copy form: a ransomware attack may make your online records inaccessible. Identify and test a fallback internal communications channel (e.g., a smartphone messaging or social media app) in case your usual systems become inoperable. Build a communications strategy that identifies which audiences need to be informed, and by whom, based on the severity and stage of the attack: IT and security operations and management; executive leadership; legal and compliance teams; partners and customers; the press and the public; regulatory authorities; bankers and investors, etc. Test the plan regularly with both tabletop and live exercises. Collect forensic data in the wake of an attack, use it to identify and close the vulnerabilities that enabled the breach, and update the response plan accordingly.

Conclusion

Any business that hopes to reduce its risk from the growing threat of ransomware must get aggressive on defense but also plan for the probability that an attack will succeed. To counter ransomware threats that are growing in frequency and sophistication, business leaders must focus their defense and mitigation planning on processes and technology that reduce overall complexity and strengthen their IT staffers with the use of AI, automation and integration.

Resources

Acronis Cyberthreats Report: Second Half of 2022
https://www.acronis.com/en-us/resource-center/resource/726/

Global Cyber Protection Landscape in 2022: Key Trends and Gaps
https://www.acronis.com/en-us/resource-center/resource/721/

Acronis Cyber Protect
https://www.acronis.com/en-us/products/cyber-protect/

Acronis

Learn more at
www.acronis.com