RANSOMWARE ATTACK CHECKLIST

CENTRIPETAL

What To Do If You Are Hit By a Ransomware Attack

Ransomware attacks were involved in 24% of all data breaches globally, nearly one in every four.[1]

High-profile attacks on governments, banks, and critical infrastructure often make the news, but small and mid-sized organizations are no less at risk of ransomware, with cybercriminals now shifting their campaigns to fly under the radar of law enforcement .

While reports frequently focus on the regularity and consequences of ransomware attacks, businesses can be left unsure of exactly what to do if they spot the signs of one. If you find yourself in this scenario, it's important to act fast and not to panic.

We've prepared a simple Ransomware Attack Checklist to help guide you in planning your response. By following this checklist, you can notify the right bodies immediately, minimize the damage to your business, and better prepare your team for future threats.

1

Validate that the alert is not a false positive

False positives occur when a scanning tool, web application firewall (WAF), or intrusion prevention system (IPS) incorrectly flag a security vulnerability during software testing. False positives describe the situation where a test case fails, but in actuality there is no bug and functionality is working correctly.

2

Isolate all infected systems

Identify and isolate all infected systems (mapped by known indicators of compromise) and disconnect all data backups from the network. Notify employees about any emails, links, or attachments that led to the attack.

3

Identify the key aspects of the attack

Collect the relevant log files, identify the initial attack vector, and inventory all infected machines. Hire a 3rd-party Incident Response team if expertise doesn't exist internally.

4

Notify law enforcement

Notify your IT security team. Your IT team should immediately be notified so they can contain the spread of the ransomware and put in place the correct procedures to deal with the attack.

Notify the authorities. It's crucial for police investigation and to prevent further incidents. Under GDPR, if you handle EU citizens' data, inform the ICO within 72 hours of a breach. Non-compliance can lead to fines up to 4% of global turnover or 20 million euros. Similar laws like CCPA apply in the US.

5

Remediate and restore the affected assets

Fix the initial attack vector to prevent re-compromise. Re-image and validate the security of all compromised systems with automated scanning software. Restore all the copies of affected files from clean backups. Scan all systems again to ensure they are clean, then reconnect them to the network.

6

Review lessons learned and make adjustments

Conduct a post-mortem on the incident to improve the organization's defenses, processes, response, and training.

[1] https://www.verizon.com/business/resources/reports/dbir/

[2] https://www.itpro.com/security/ransomware/361853/ransomware-groups-will-target-smaller-businesses-in-2022