5 Critical Steps to Recover From a Ransomware Attack

June 21, 2021 The Hacker News

(https://thehackernews.com/images/-25giPdrESEI/YNCfZZzKV7I/AAAAAAAABDs/mWDOej6y-yA50gsfkJqrs5bdC7on2kxiQCLcBGAsYHQ/s0/ransomware.jpg)

Hackers are increasingly using ransomware as an effective tool to disrupt businesses and fund malicious activities.

A recent analysis by cybersecurity company Group-IB revealed ransomware attacks doubled in 2020 (https://www.group-ib.com/resources/threat-research/ransomware-2021.html) , while Cybersecurity Ventures predicts that a ransomware attack will occur every 11 seconds (https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/) in 2021.

Businesses must prepare for the possibility of a ransomware attack affecting their data, services, and business continuity. What steps are involved in recovering from a ransomware attack?

- Isolate and shutdown critical systems
- Enact your business continuity plan
- Report the cyberattack
- Restore from backup
- Remediate, patch, and monitor

Isolate and shutdown critical systems

The first important step is to isolate and shut down business-critical systems. There is a chance the ransomware has not affected all accessible data and systems. Shutting down and isolating both infected systems and healthy systems helps contain malicious code.

From the first evidence of ransomware on the network, containment should be a priority. Containment and isolation can include isolating systems from a network perspective or powering them down altogether.

Enact your business continuity plan

The business continuity plan and its disaster recovery component are essential to maintaining some level of business operations.

The business continuity plan is a step-by-step playbook that helps all departments understand how the business operates in times of disaster or other business-altering scenarios. The disaster recovery component details how critical data and systems can be restored and brought back online.

Report the cyberattack

Many businesses may hesitate to do so, but reporting the attack to customers, stakeholders, and law enforcement is essential. Law enforcement agencies can

provide access to resources that may not be available otherwise.

You will also need to consider compliance regulations. The GDPR, for example, provides businesses with a 72-hour window to disclose a data breach involving customers' personal information.

Restore from backup

The best protective measure you have for your data is backups. However, restoring large quantities of data can be time-consuming, forcing the business to be offline for an extended period of time.

This situation highlights the need to discover and contain ransomware infections as quickly as possible to reduce the amount of data that needs recovering.

Remediate, patch, and monitor

In the final phase of recovering from a ransomware attack, companies remediate the ransomware infection, patch systems that may have led to the initial ransomware compromise, and monitor the environment closely for further malicious activity.

It is not unheard of for malicious activity to continue, even if the ransom is paid, or if infected systems were restored. If the same vulnerability exists that led to the initial attack, the environment can become compromised once again.

Remediate common entry points for ransomware

As businesses look to bolster the environment against ransomware and other malicious threats, it is crucial to look at the common entry points for these types of attacks.

Cyberattacks use phishing attacks to harvest stolen credentials which can then be

used to launch a ransomware attack, or access systems directly.

Prevention and next steps

Businesses must not be careless in handling password security, especially with Active Directory user accounts. Unfortunately, Active Directory does not have good native security tools for securing passwords in line with today's password security policy requirements.

Specops Password Policy provides breached password protection, disallowed password lists, and many other robust security features to protect your environment. It takes the very basic password policies available in Active Directory and aligns them with modern guidance from NIST and other cybersecurity authorities.

Learn more about Specops Password Policy and download a free trial (https://specopssoft.com/product/specops-password-policy/?utm_source=hackernews&utm_medium=referral&utm_campaign=HackerNews%20blog) to protect your environment from vulnerable passwords.

Found this article interesting? Follow THN on Facebook (https://www.facebook.com/thehackernews) , Twitter (https://twitter.com/thehackersnews) and LinkedIn (https://www.linkedin.com/company/thehackernews/) to read more exclusive content we post.