How To Recover From A Ransomware Attack? 5 Top Tips

Ransomware attacks against healthcare organisations have jumped about 45% since early November, following an alarming 71% increase in October 2020, making healthcare the number one target of ransomware attacks that month. Fending off these attacks can be incredibly difficult, but it's not impossible. HealthManagement offers several best practices from IT experts.

Ransomware attacks on US healthcare organisations cost an estimated $21 billion in 2020. During the year, 92 individual ransomware attacks affected over 600 separate clinics, hospitals, and organisations and more than 18 million patient records.

What Is Ransomware?

There are two main types of ransomware: crypto-ransomware and locker-ransomware. Crypto-ransomware encrypts an organization's data and demands a ransom in order to have the files decrypted and safely returned. Locker-ransomware works in much the same way, except that it prevents users from accessing the files instead of encrypting them, before demanding a ransom for the data to be "unlocked". In both cases, the attacker demands payment, threatening to publish sensitive information or permanently remove data from the system if the victim fails to pay up.

How does ransomware get onto your system in the first place?

It often starts with a trojan. A trojan is a type of malware that tricks victims into thinking it's harmless by disguising itself as legitimate software. Trojans are primarily spread through spam mails. If the recipient opens the attached file or clicks on the URL, they unknowingly download the trojan, which then has the power to steal sensitive data. But attackers can *also* use it to spread other malware, like TrickBot or Qbot. This second layer of malware then spreads laterally through the company, stealing credentials, deploying backdoors and, perhaps most importantly, trying to access the domain controller. If they succeed in accessing the domain controller, the attacker can then deploy ransomware such as Ryuk, which encrypts the organiation's data and demands the ransom. Some ransomware, however, doesn't require user interaction to spread. Worms like WannaCry are a type of malware that replicate themselves so that they can tear through a system like wildfire, without the need for someone to keep passing it on via malicious URLs or attachments.

How Can You Recover From A Ransomware Attack?

1. **Don't pay the ransom.**

First things first: don't pay the ransom unless you haven't got any copies of your data stored elsewhere at all, in which case you need to weigh up the cost of the data loss vs the demanded payment. A recent survey found that 26% of ransomware victims had their data returned after paying the ransom, and 1% paid the ransom, but didn't get their data back. 56% of victims, more than twice as many as those who paid the ransom, recovered their data through backups.

2. **Report the attack.**

This will help authorities identify the attacker and how they're choosing their targets, and help prevent other organisations from falling victim to the same attack. Generally, you can contact your local police, who will put you through to their cybercrime investigations department. If in the US, you can also report via the On Guard Online website; in the UK, through Action Fraud.

3. **Cleanse your systems.**

There are some software packages available that claim to be able to eradicate ransomware from your systems, but there are two problems with this. The first is that you can't be sure that anyone other than the attacker will be able to completely remove the ransomware. The second is that, even if your system is successfully cleansed, you still may not be able to access your data. Unfortunately, there isn't a decryption tool for every type of ransomware out there, and the newer and more sophisticated the ransomware, the more time it will take experts to develop a tool to unscramble your files. Encryption involves running a decryption key and the original file through a function together to recover the original file. However, modern attacks use a unique key for each victim, so it could take years for even a powerful supercomputer to find the right key for an individual victim.

4. Restore your data.

Data backup is traditionally considered an IT compliance issue, carried out to tick boxes and get through audits. However, it's becoming increasingly viewed as a security topic, and for good reason.

"Preventing a cyberattack isn't always possible, but mitigating the impact certainly is, which is why backup should be considered a security issue," Seymour explains. "Once an organisation becomes a ransomware victim, it's faced with a dilemma: pay the ransom, which is never advised, or move forward without the data. If the organization has a proper backup strategy in place to counteract cyberattacks, it can quickly recover by accessing its backed up data and avoid costly downtime."

5. Prevent a repeat attack

Endpoint detection and response (EDR) solutions continuously monitor all incoming and outgoing traffic on a network for potential threats. If a threat is detected, the solution isolates the affected machine so that the malware can't spread. But here's the important part: EDR doesn't just keep a record of the incident itself, but of all the events that led up to the incident, too. This means that you can see which files, processes and registry keys the hacker accessed, and identify where the attack started and how it progressed. You can then use this information to stop the same incident from occurring again.

Source: TechRepublic
Photo: iStock

Published on : Tue, 6 Jul 2021