



Recovering From a Ransomware Attack



A ransomware attack can cost businesses a great deal. The effects of an attack are devastating, as many companies can fall into a profound financial loss. Once a ransom attack is made known, customers' trust will be broken, and they will flee to competitors. As information is more digitized, the chances of an attack grow. To prevent an attack, businesses should be prepared with [backup and disaster recovery solutions](#).

Defining a Ransomware Attack

A ransomware attack is when software makes its way into a computer and then demands a fee in order to release the hacked files. Unknown links in emails, messages, or websites can increase the chances of a ransomware attack. These links are generally encrypted with important information and files that lock the computer's data. Once



the fee is paid, the attackers unlock your files. Ransomware has evolved along with technology, and now attacks can occur in network drives and backup data. Ransomware has the ability to ruin data copies that are unable to be recovered with recovery services. Efficient training on avoiding messages and websites that might be bait is imperative, along with security tools.

Preventative Measures

To prevent ransom attacks, a multi-layered backup protection solution can assist in keeping information safe. However, there is more that must be done. As ransomware evolves, IT equipment must evolve with it.

Protect Backup Data

A multi-layer approach that strategically assists in preventing your backups from ransomware attacks is vital. Strict access control is essential, including role-based access control and multi-factor authentication solutions.

Detect Ransomware Attacks

Automated monitoring and machine learning assist in providing algorithms that scan for anomalies. With these systems, ransomware is discovered and flagged.

Recover Rapidly and Cleanly



Disaster recovery solutions are imperative. A dashboard that efficiently shows the health status and vulnerability of a backup is vital.

Good Anti-ransomware

When investing in anti-ransomware, it is essential to search for one that is reliable. Ensuring that the solution offers a clean and quick recovery solution is vital. Being able to see your data and check for issues before restoring is also crucial. Immutable backups, strict access controls, machine learning aided detection, and instant mass restores are all important solutions.

General Benefits

Anti-ransomware software provides reassurance that a business will not be held ransom. If attackers attempt to breach primary defenses, a backup solution integrated with anti-ransomware capability can reduce damage and prevent massive data loss. Businesses can breathe if they choose Pathway's cloud backup in Canada. Our disaster recovery services will deliver customizable backup and recovery services suitable to your business. Minimize downtime and interruptions when turning to professionals. For more information, [contact us](#) today.

Original Source Link:

<https://medium.com/@michaelmiller8/recovering-from-a-ransomware-attack-581f53c27fc3>