DATA BACKUP IS NOT ENOUGH
YOU ALSO NEED DATA PROTECTION

WHAT TO LOOK FOR IN A DATA PROTECTION BACKUP SYSTEM

IT SOLUTIONS
By Rob Landis, Binary IT Solutions

The need to back up data has been around since floppy disks. Data loss happens due to viruses, hard drive crashes, and other mishaps. Most people using any type of technology have experienced data loss at least once.

But one thing that's changed with data backup in the last few years is security. Simply backing up data so you don't lose it, isn't enough anymore. Backing up has morphed into data protection.

Some of the modern threats to data backups include:

• **Data Center Outage:** The "cloud" basically means data on a server. That server is internet accessible. Those servers can crash. Data centers holding the servers can also have outages.

• **Sleeper Ransomware:** This type of ransomware stays silent after infecting a device. The goal is to have it infect all backups. Then, when it's activated, the victim doesn't have a clean backup to restore.

• **Supply Chain Attacks:** Supply chain attacks have been growing. They include attacks on cloud vendors that companies use. Those vendors suffer a cyberattack that then spreads throughout their clients.

• **Misconfiguration:** Misconfiguration of security settings can be a problem. It can allow attackers to gain access to cloud storage. Those attackers can then download and delete files as they like.

What to Look for in a Data Protection Backup System

Just backing up data isn't enough. You need to make sure the application you use provides adequate data protection. Here are some of the things to look for when reviewing a backup solution.

Ransomware Prevention: Ransomware can spread throughout a network to infect any data that exists. This includes data on computers, servers, and mobile devices. It also includes data in cloud platforms syncing with those devices.

Continuous Data Protection: Continuous data protection is a feature that will back up files as users make changes. This differs from systems that back up on a schedule, such as once per day.

Threat Identification: Data protection incorporates proactive measures to protect files. Look for threat identification functions in a backup service. Threat identification is a type of malware and virus prevention tool.

Zero-Trust Tactics: Cybersecurity professionals around the world promote zero-trust security measures. This includes measures such as multi-factor authentication and application safelisting.

Backup Redundancy: If you back up to a USB drive or CD, you have one copy of those files. If something happens to that copy, you could experience data loss. Cloud backup providers should have backup redundancy in place. This means that the server holding your data mirrors that data to another server.

Air Gapping for More Sensitive Data: Air gapping is a system that keeps a copy of your data offline or separated in another way.

Need Help With Secure Backup & Data Protection Solutions?

Have you updated your backup process for today's threats? Give us a call today to schedule a chat about data backup and protection.

Rob Landis can be reached at 610-320-2628. Binary IT Solutions is a Managed Service Provider supporting small to medioum sized business with teir business IT needs. Find more information at www.binaryitsolutions.tech