Publication: Hi-Tech Security Solutions
Title: How safe are your backups?
AVE: 39352.5

Page: 29
Publish Date: 01 September 2022
Author: Andrew Seldon

How safe are your backups?

By Andrew Seldon.

Immutable backups prevent malware from compromising your data and ensure the right data is restored in an emergency.

Any terms relating to cybersecurity today invariably focus on the information technology aspect, specifically the elements that get the most attention, such as malware, ransomware and hacking. While all of those are critical, it's easy to forget about cyber resilience.

Cyber resilience, as this feature shows, includes the above, but goes much further. Backups used to be something companies had to do in case their IT infrastructure failed, such as hard drive crashes, etc. However, taking ransomware as an example, we can see how important backups are when you suddenly find your data encrypted and held to ransom.

Unfortunately, cybercriminals are aware that it may be easier for companies to restore a backup rather than pay the extortion money, and have adapted to this circumstance. Today, ransomware (and other malware) may reside on companies' servers for weeks or even months before it is triggered, to ensure that the data which is supposedly safe and backed up is infected or encrypted and can't be restored.

We also know that data may be stolen and even if the company pays up (one or more times), it can still be sold to the highest bidder. Moreover, it is said that a cyber breach takes an average of 287 days to identify and contain, which means even backups made a month or a quarter ago may be corrupted. Even if those backups are fine, this ignores the fact that the data is old and whatever transpired in the meanwhile is lost forever.

Hi-Tech Security Solutions spoke to Hayden Sadler, country manager at Infinidat, about the backup problem to find out what solutions are available to protect data and to ensure 'clean' data is available to restore when something happens.

Time to restore

Sadler believes backups remain a critical part of any IT and cyber resilience programme, however, the time it takes to restore the data is often neglected. It can take days or weeks to restore the data and applications for large companies, which is often as long or longer than the disruption caused by the breach. A cyber resilience process therefore needs to ensure protection as well as fast recoverability.

The traditional 3-2-1 backup standard, where there is one primary backup and two copies are made on different types of media – and one stored offsite – will therefore not help in a case where the criminals have been in your network for a long time. Sadler advises every company to design its backup process based on the following four pillars:

1. They need an immutable (unchangeable) snapshot of their data. This system should also have integrated anomaly detection to immediately warn if the data is infected with any type of malware.
2. It needs to be 'air gapped', meaning it is not stored in the same area or network as the original data. (Having a directory named 'backups' on the server doesn't really help.) In the past, tape backups were the natural way of air-gapping backups, but the restore times can be lengthy and there is generally no way to ensure the tapes are malware-free.
3. Companies need a safe environment to restore and test backups to avoid restoring malware and to make sure the restoration works properly.
4. They need to be able to restore their data almost immediately.

Triple redundancy

Infinidat offers customers a triple-redundant architecture where it mounts an immutable snapshot (or a separate server) using a separate physical network. This allows snapshots to be tested before being stored and offers a safe environment to restore to before overwriting your data.

The company's InfiniGuard solution is equipped with InfiniSafe to ensure cyber protection at the highest levels at no additional cost. InfiniSafe's comprehensive cyber storage resilience approach provides rapid recovery into production. Sadler cites an example where a 1,5 PB Veeam backup dataset was restored in just over 12 minutes.

Hayden Sadler.

The company says InfiniGuard solutions can scale up to an effective 50 PB of data and support multiple protocols (such as VTL, NFS, CIFS, OST, RMAN and DB2), with "in-line ingest rates of up to 180 TB per hour." Apart from the rapid recovery capability, its InfiniBox architecture also provides multiple levels of data protection, including role-based access control and multi-factor authentication, at-rest encryption, encrypted replication, the above-mentioned isolated storage via immutable snapshots, and more.

Infinidat recently announced an expansion of its guaranteed service level agreement (SLA) programme, the industry's first cyber storage guarantee for recovery on primary storage – the InfiniSafe Cyber Storage Guarantee. It ensures that enterprises and service providers recover and restore their data at near-instantaneous speed in the wake of a cyberattack by using a guaranteed immutable snapshot dataset with a guaranteed recovery time of one minute or less.

Infinidat operates in South Africa via channel partners, but the company is involved directly with customers to ensure they understand what is required and how InfiniBox, InfiniGuard, InfiniSafe and the related enterprise storage solutions can effectively provide modern data backup services, as well as cyber resilience.

For more information contact Infinidat, scapoor@infinidat.com, www.infinidat.com