Publication: Electricity and Control
Title: Safe data storage and effective recovery
AVE: 21635.4

Page: 30
Publish Date: 01 October 2021
Author: Lourens Sanders

CYBERSECURITY

Safe data storage and effective recovery

Lourens Sanders, Solution Architect at Infinidat

Lourens Sanders, Infinidat.

South Africa is an attractive target for cybercriminals for a number of reasons, and the past few years (and months) have seen a sharp rise in high-profile ransomware attacks. One of the key drivers of increasing attacks is the fact that data is a de facto currency and a valuable commodity on the black market. While backup is a critical component of data protection, when this backup is also encrypted by malicious software, companies are often left with few options other than to pay the ransom. That means an effective cyber recovery strategy is key to enabling businesses to get back up and running without having to give in to criminal demands.

Ransomware on the rise

The rapid adoption of digital transformation, artificial intelligence, and the Internet of Things (IoT) has left vulnerabilities in cybersecurity. In the context of the pandemic, it has been a challenge to roll out new technology and address the specific aspects of security that should be done at the same time.

This has made some local businesses appealing targets for strategic attacks. According to Kaspersky, South Africa ranks third in the world for the highest number of users experiencing targeted ransomware attacks. There was a striking increase in targeted ransomware between 2019 and 2020, although general ransomware attacks decreased.

Another concerning trend highlighted by Kaspersky is that 42% of ransomware targets in South Africa paid a ransom in the hope of getting their data back, because they do not have the appropriate systems in place to recover on their own. And although almost half of the victims surrender to paying the ransom, less than half get their data back, which perpetuates the cybercrime cycle.

A comprehensive cyber recovery strategy should provide numerous options for data restoration.

Backup solutions have been the mainstay of data protection for many years, but they are no longer sufficient. Standard backups do not provide a high level of granularity and they can take some time to recover. They also present only a one-dimensional approach to data protection. If that data is corrupted, infected or otherwise compromised, businesses are left stranded. Cybercriminals are increasingly targeting backup solutions, so although data backups remain essential, they are of no use in a targeted ransomware attack because the backups themselves are likely also encrypted and held for ransom.

A holistic recovery strategy

When a data loss event occurs, for whatever reason, the goal is to restore a business to an operational state, where key applications and services are made available, as quickly as possible. Without a holistic strategy, which addresses security gaps and allows businesses to recover their data, mitigating the risk of a ransomware attack is all but impossible.

A comprehensive Cyber Recovery strategy should provide for numerous options for recovery from multiple copies of your data, including snapshots, clones, replicas, or actual backups. This not only addresses the need for enhanced granularity when backing up and recovering, it also protects key applications and services. It enables recovery in the shortest timeframe possible, with multiple recovery points to work from. Furthermore, a thoroughly implemented strategy ensures your data protection environment will not be compromised by ransomware.

Restoration is key

The ability to restore data in the case of loss, damage or compromise, especially from a cybersecurity related incident, is essential to business continuity. Ransomware fees and downtime can sink a business, whereas with an effective restoration and recovery strategy, the impact is minimised because there is always a validated, uncompromised copy of data available.

Today, more than ever, it is critical to adopt best practice around data protection, incorporate processes that validate backups and test restores, and ensure proactive monitoring and alerting to detect anomalies. Purpose-built data protection technologies offer the ability to protect production data, and keep those copies safe and reliable for recovery – a critical requirement in a world where cybercrime is on the rise.

For more information visit: www.infinidat.com