BIZCOMMUNITY

How businesses can recover from ransomware attacks

By Lourens Sanders

17 Sep 2021

South Africa is an attractive target for cybercriminals for a number of reasons, and the last few years have seen a sharp rise in high-profile ransomware attacks. One of the key motivations driving this volume of attacks is the fact that data is a de facto currency and an extremely valuable commodity on the black market.

Lourens Sanders, solution architect at Infinidat | image supplied

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. Therefore, an effective Cyber Recovery strategy, which enables businesses to get back up and running without having to give in to criminal demands, is the key.

Ransomware on the rise

The rapid adoption of digital transformation, Artificial Intelligence (AI) and the Internet of Things (IoT) has left vulnerabilities in security. In the wake of the pandemic, it has been a challenge to roll out cutting-edge technology, while also addressing the specific aspects of security that should be done in conjunction.

As a result, this has made 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 767% increase in targeted ransomware from 2019 to 2020, while general ransomware attacks decreased by 29%.

Held to ransom

Another concerning trend highlighted by Kaspersky is that 42% of ransomware victims 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. While almost half of the victims surrender to paying the ransom, less than half get their data back, which perpetuates the cybercrime cycle.

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 can also take some time to recover.

Kaspersky records over 2m phishing attacks in SA in H1 2021
14 Sep 2021

They are also 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 also encrypted and held to ransom.

Holistic, strategic

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 is necessary to allow 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.

This enables recovery in the shortest time frame possible, with multiple recovery points to choose from. Furthermore, a thoroughly implemented strategy ultimately ensures your data protection environment will not be compromised by ransomware.

Restoration is the key

The ability to restore data in the case of loss, damage or compromise, especially from a cyber security-related incident, is essential to business continuity. Ransomware fees and downtime could end up sinking 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 practices around data protection strategy, 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 not only to protect production data but keep those copies safe and reliable for recovery – a critical requirement in a world where cybercrime is on the rise.

ABOUT THE AUTHOR

Lourens Sanders is a solution architect at Infinidat.