CASE STUDY

THE POWER OF PROFESSIONAL REPLICATION AND BACKUP

When it fell victim to a devastating ransomware attack, this ContinuitySA client found out the hard way that all disaster recovery is not equal.

The client is a large services organisation, wholly reliant on its 24/7 call centre to receive and schedule client service requests. The majority of the service requests are urgent and relate to a range of emergency services.

This large service organisation fell victim to a ransomware attack using Samsam Prosperity 666 which had only been released 2 days prior to the attack. All its IT systems and data, including their telephony system, were encrypted by the ransomware app, and a large ransom in Bitcoin was demanded before the organisation's systems and data would be unlocked. The organisation took the decision not to capitulate to the illegal ransom demand, and invoked a disaster with ContinuitySA, its long-term business resilience partner.

Later investigation showed that the cyber criminals exploited a temporary vulnerability when the organisation's firewalls were upgraded and a security patch was not updated sufficiently quickly a clear indication of how efficient these criminal syndicates are, and also that the organisation had probably been under long-term surveillance.

Because of the nature of its business, the first imperative was to shut down the network links between the client's site and ContinuitySA, to isolate the recovery facility and prevent the ransomware app spreading to the recovery site. The next priority was to get its call centre up and running. The majority of its servers were replicated at the ContinuitySA data centre and were able to be brought up within a short time. Once the client's staff had been relocated to the ContinuitySA data centre in Midrand, it was able to continue operating while its production environment was rebuilt.

Crucially, since ContinuitySA uses Veeam with Exagrid technology as the backup target for server backup, these backup's were unaffected by the ransomware. The Exagrid/Veeam technology creates an "air gap" between the production systems and the backed up data to prevent malware damaging the backups.

To save costs, the client had elected to do its own backup for a group of servers hosted at a third-party data centre to an ordinary network NAS drive. Unfortunately, these backups were not protected by the same technology and were compromised by the ransomware. This group of servers and their backups could not be recovered which resulted in a loss of data that had a substantial financial impact.

As cyber-attacks, particularly ransomware attacks, become more frequent and sophisticated, it is essential that replications and back-ups are adequately quarantined from malware. Keeping backups / replications in a sanitised, protected environment is clearly critical, and emphasises the imperative for organisations to partner with a specialist business resilience and continuity provider like ContinuitySA, with access to leading-edge technology and processes.

Our Business is keeping You in Business

Continuity sa

+27 11 554 8000 / info@continuitysa.co.za / www.continuitysa.com