Don't cry over data loss as a result of WannaCry if you could have prevented it

- *Security practitioners the world over should take a stern reality check after WannaCry ransomware hits the globe*

The WannaCry ransomware cyber attack orchestrated over the weekend of the 12th of May should act as a stark reminder to companies that data backups need to be done regularly, that security solutions have to remain up to date and that user education is still a vital component of every security policy.

This is according to Andrew Potgieter, Security Solutions Director at Westcon-Comstor Southern Africa, who adds that even more unnerving is that "kits" to put together attacks of this nature are readily available for download on the Internet and doesn't require a group of elite hactivists to run.

"Ransomware encrypts the data in your data centre (storage) or on personal devices and holds it 'ransom' until you pay the fee requested by the 'data kidnapper'. What made the WannaCry attack so different is that it was done on a global scale, spreading to 150 countries, impacting over 10,000 organisations and 200,000 individuals – exploiting a security flaw in Windows XP," states Potgieter.

Furthermore, he says that perhaps the most startling component of the attack is that so many companies were simply crippled. Highlighting that there is a real flaw in IT security policies, there are few organisations with effective "crisis situation" policies in place and that companies who simply fall back on two-dimensional, anti-intrusion detection and prevention methods will continue to fall victim.

Simply put, according to Westcon-Comstor vendor partner AlienVault, WannaCry is a ransomware variant that takes advantage of an exploit in the Windows operating system (MS17-010) that was released by a hacking organisation called Shadow Brokers in March. The exploit and tools were allegedly part of a collection of spy tools used by the National Security Agency (NSA). While Microsoft patched the vulnerability pretty quickly after the release, many clients have not run the updates needed to deploy the latest patch. Once an infected computer is put into action the malware spreads like a worm on your network, sniffing out other vulnerable machines to infect.

Regular backups and snapshots can help you recover files hidden behind ransomware, particularly if you can identify when the infections occurred, so you only work with backup copies before the infection. While you won't be able to recover your files since the last backup, without paying the ransom, you can get at older files that are critical to business operation and continuity.

"Ransomware hides your data, but that data can be restored if regular backups are done in a business. Backups shouldn't just be a business imperative, but a security one too, as all data needs to be continually and regularly scanned and cleaned of hidden malware. Updates might be a pain and slow your machine, but there are critical in a business, you simply have to run all updates as often as you can. It is the job of the IT department to ensure this happens.

"This is a huge wake up call for security practitioners, software developers and businesses alike. One small vulnerability can cripple your business. It is not just IoT and digital platforms that are affected it is all platforms. If businesses weren't aware that they need to take security seriously, then this attack should surely change their minds," ends Potgieter.