Ransomware: African businesses continue to be at high risk

Over the last 12 months, there has been a 16% increase in ransomware attacks, a Data Breach Investigation Report by Verizon, has revealed.

Image by 123RF

Ransomware is a hot topic because of the organisations being targeted and because of how prevalent it has become. The report revealed that 89% of attacks “involve financial or espionage motivations”, with the former a clear catalyst.

While every single individual is at risk to a ransomware attack, there is certainly a higher degree of risk attached to businesses, more so those that handle confidential and sensitive information, for whom the effects of ransomware could be devastating from both a financial and reputational perspective.

Interestingly, the study noted how phishing is a growing concern, as it is evident a lot of people are not familiar with this tactic. For example, Verizon found that 30% of phishing messages were opened in 2015, which is up a massive 23% from 2014.

Phishing has been used by cybercriminals for years to access personal information. It can manifest itself as an email, text message or even a website.

Steve Flynn, director of ESET South Africa advises companies to, “Backup, backup, backup. This may well be your saviour when faced with a ransomware outbreak in your organisation. Have an external backup that runs daily and make sure that you unplug the backup when it is not running, otherwise, it may also be encrypted.”

Despite advances in information security research and cyber detection solutions, we continue to see many of the same errors that we have known about for a decade or so.

The author of the report highlighted a “three-pronged attack”, which is, “being repeated over and over again” by cybercriminals.

It begins with a phishing email that comes with a link to either a corrupted website or attachment. On clicking through to a website or attachment, malware is downloaded onto a victim’s computer. This “establishes an initial foothold”, meaning that further malware can be downloaded to either encrypt data, access information and/or steal credentials. These credentials are used to carry out further cybercriminal activity, including breaching bank accounts.

Flynn also recommends organisations to implement IT admin policies around email attachments. “Network admin should enforce strict rules around allowing users to receive only necessary attachments, and furthermore, not allow, or impose conditions around personal emails on the organisational network.”