Growing threat of ransomware in SA needs immediate action, says Ispa

There's no time like the present and with local firms increasingly in the sights of organised cyber criminals, SA's Internet Service Providers' Association (Ispa) says ransomware defences must be routinely evaluated and disaster recovery procedures regularly tested.

Source: Pixabay

Best practice demands three copies of backup data with two copies onsite, on different media, and at least one copy offsite.

With the average cost of remediating a ransomware attack in SA estimated last year by cybersecurity firm Sophos to be R6.4m, there are significant financial and legal risks to exposure to the online realm.

Specifically, it is tremendously risky not to immediately patch known vulnerabilities targeted by organised cybercriminals.

Ransomware is an increasingly common type of malware that infects a target and threatens to restrict access until a ransom is paid or publish a victim’s confidential data. Ransomware is mostly designed with a mechanism for the victim to pay a ransom to access their data or secure the attacker’s silence.

According to Ispa chair, Sasha Booth-Beharilal, cybercrime disrupts more than business operations, it exposes

organisations to reputational and regulatory risk. Not only are ransomware attacks becoming more frequent, but developments overseas are suggesting that policing agencies globally are not considering the payment of ransom as a mitigating factor when considering enforcement actions. This, again, underscores the importance of a proactive approach to cybersecurity.

Ensuring industry-accepted best practice principles are followed helps to protect against cybercriminals and their ransomware demands.

Ispa says some key principles here include:

- The adoption of IT policies such as the Principle of Least Privilege (PoLP) and Segregation of Duties (SoD) across your business. This is applicable to user access as well as network architecture.
- With the PoLP, a multi-layered network design is best. With a VPN concentrator or bastion host, this design should secure your vital management network behind these hardened public-facing endpoints and aim to reduce the external threat surface.
- Ensure that regular penetration testing is performed. The results should be conveyed to executive management, with corrective measures tracked on a roadmap. This should allow improved IT governance and executive support in correcting the identified shortcomings.
- While a penetration test is a thorough security assessment, it can often be too infrequent. With technical changes happening at a rapid pace and new exploits being discovered more frequently, an effective real-time monitoring solution such as a vulnerability management platform is advisable to supplement the penetration testing intervals.
- A vulnerability management tool creates an objective perspective on your security posture. This in turn should reflect the software update cadence in your environment by highlighting known vulnerabilities. Implementing a software update or patching policy should formalise and instil this concept as part of the operating processes of the organisation.
- Legislative imperatives should not be overlooked when it comes to cybersecurity. In terms of the Protection of Personal Information Act 4 of 2013 (PoPIA), businesses are required to mitigate risk relating to the processing and storing of personal information. PoPIA specifically requires organisations to implement reasonable technical and organisational measures in this regard.

Ispa also advises of the importance of regular training and organisation-wide awareness initiatives aimed at sensitising employees, business partners and others to the fact that the human element is often the weakest cybersecurity link. Phishing via phone and email remains a particular concern in the context of ransomware.

It should be remembered that both businesses and consumers must always report cybercrime as they would any other crime. When reporting a cybercrime at a local South African Police Service station, it is imperative that the complainant requests that it be forwarded to the police’s Cybercrime Division.