SA is a target for cyber attacks

The digitisation of our personal and work lives is making society increasingly reliant on technology, and more vulnerable to the risk of a debilitating cyberattack. With the accelerating pace of technological change, attacks a continuously intensifying in frequency and severity. Data breaches, the theft of business-critical information and ransom demands are all threatening the reputation and stability of businesses.

Source: pixabay.com

The World Economic Forum recently listed cybersecurity as the fifth highest global risk for doing business, and IT is considered the top risk in Europe, North America and East Asia. South Africa is becoming a major target for cyber attack

According to the South African Banking Risk Information Centre (SABRIC), the country has the third highest number of cybercrime victims worldwide - losing around R2.2bn a year to cyber attacks.

New sophisticated methods of attack include targeting essential infrastructure, co-operation between attackers, the use of artificial intelligence and remote access takeovers through Internet of Things (IoT) devices. Small businesses are particula at risk, with cyber defences that are easier to breach.

Creating threat awareness and cyber resilience

As 5 February marks Safer Internet Day, Heino Gevers, a security specialist at Mimecast, suggests businesses protect themselves against a potentially devastating cyber attack, by implementing a robust cyber resilience strategy. Nine of out t data breaches start with email, so it's important to not only prevent email-borne cyber attacks but to be able to recover fror them as well.

This can be achieved by having the right advanced security services in place before an attack happens, continuity during attack and the ability to recover data after an attack. Additionally, organisations should improve their defences by reducing human error with an effective user awareness training programme.

CYBERSECURITY

Become more cyber smart in 2019

29 Jan 2019

Another essential defence mechanism is making use of threat intelligence. Security leaders should use data from multiple internal and external sources and use it to identify emerging threats, unearth the conditions needed to exploit vulnerabilities and discover whether the threat is being actively used. While this has previously been the reserve of large, well-funded organisations, threat intelligence is increasingly becoming accessible and affordable to most businesses.

A cyber security strategy

After an attack, it can be difficult, if not impossible, for a business to recover without the correct solutions in place. According to King Price's Wynand van Vuuren (partner of client experience) combining a proactive security approach wi a strong cyber insurance policy is essential for any business to guard against the potential cost of restoring productivity a reputation.

Proactive security measures include implementing firewalls, appropriate security software, malware scanning and continu employee training on the basics of security.

While a cyber insurance policy can't prevent your company from being attacked, it is an important way to protect businesses from the after-effects of a breach.

King Price's cybersure policy covers:

- Data breach expenses, including cover for the costs of hiring legal and forensic IT professionals to help you recover your data.
- Damage to computer systems and data.
- Disruption following a cyber attack can bring certain systems and applications to a halt, affecting productivity.
- Liability and reputation management costs following a cyber attack.