5 ways your small business can strengthen its cybersecurity defence

By Clement Sibiya

26 Apr 2024

Despite the many benefits of cloud computing, it also brings new complexities to cybersecurity for South Africa's small and medium enterprises (SMEs).

Source: Unsplash

They have embraced cloud services to take advantage of scalable subscription services that enable hybrid working models, allowing them to turn IT from a capital cost into operational expenditure, and achieve higher levels of flexibility.

The public cloud services and applications SMEs source from providers like Microsoft, AWS and Google are hosted in secure data centres. But end-user devices used to access these services—such as PCs and smartphones remain vulnerable to a range of threats—including malware, insider data theft, ransomware and elaborate social engineering threats.

Global research from Sage found that half of SMBs have experienced a cybersecurity incident in the past year and a quarter have experienced more than one. A Sophos study meanwhile found that South Africa had the biggest increase in ransomware attack rates, with 78% of organisations hit in the 2023 survey compared to 51% in 2022.

How the 'GoFetch' attack could target your Mac

Lindsey Schutters 25 Mar 2024

The risks of cyberattacks and data breaches are significant. Sophos found there was a direct revenue loss to 82% of private sector organisations in South Africa that experienced ransomware attacks.

There are also possible regulatory repercussions, with regulations under the Protection of Personal Information Act providing for stringent fines and penalties for non-compliant companies.

This is without mentioning the impact on customer relationships, possible legal liabilities, and the business costs of losing business-critical data.

With SMEs on cybercriminals' radar, it has become more important than ever to fortify their data and systems. Here are a few ways that your SME can strengthen its cybersecurity defences:

1. Consider moving towards a zero-trust model

SMEs can benefit from embracing a zero trust security model, a framework that operates on the principle of "never trust, always verify".

In practice, this means that your business will not automatically trust any person, device, or system inside or outside your network. Everyone and every device will need to authenticate before gaining access to data or systems.

Many cloud services such as Microsoft 365 Business support zero trust principles—provided they are configured correctly.

2. Remember your devices are your weak point

The physical theft or loss of a smartphone or notebook with privileged access to cloud services and apps is one of your biggest risks.

In the Sage research, the most mentioned cybersecurity incident was stolen laptops (28%). Make sure your end-users protect their devices from unauthorised access with biometric authentication (facial recognition or fingerprints) or strong passwords.

Use the 'Find My PC/Phone/Tablet' feature to improve the chances of recovering a lost or stolen device.

3. Introduce regular security training

Data breaches or malware attacks can be the result of human error. Sophisticated cybercriminals gain access to your systems or data through social engineering techniques that exploit employees' fear, ignorance, or negligence.

New SME survey results reveal upcoming national elections a deep concern for SA small business owners

Business Partners Limited 25 Apr 2024

It’s thus imperative to regularly train employees in cloud security risks and best practices. Educating users about phishing scams, data privacy, and secure cloud usage goes a long way in mitigating the risk of human error leading to security incidents.

4. Implement multi-factor authentication

Most data breaches occur because of a cybercriminal getting their hands on user credentials to access systems via the cloud. The majority of these attacks can be stopped with multi-factor authentication (MFA).

With MFA, users use a one-time password or PIN emailed or texted to them when they want to access a system. Or they could use an app like Google Authenticator or a hardware token to generate a code.

5. Plan for the worst

Prepare yourself to bounce back quickly if the worst happens. Ensure that you regularly back up any data you store in the cloud or on local devices. The best practice is to create three copies—two onsite, one offsite—to ensure the business can recover from an attack.

Also develop and regularly test an incident response plan specific to cloud security incidents. This plan should outline steps for identifying, containing, and mitigating the impact of security breaches in the cloud environment.

ABOUT THE AUTHOR

Product manager: Cloud and IoT at Nashua.