BIZCOMMUNITY

5 cybersecurity tips to secure your workforce

By Andrew Bourne

26 Oct 2021

It has been almost two years since the pandemic began, with the first lockdown in March 2020 forcing businesses to adopt a remote working approach. Now that South Africa is opening up, a hybrid model is quickly becoming the norm, with employees splitting their time between the office and their home. As a result, the IT department's role has become more complicated than ever, owing to the rapid increase in remotely connected devices. Cyberattacks have, in turn, become more common.

Image source: © Maksim Kabakou – 123RF.com

The most high-profile cyberattack happened in July, when Transnet, the state-owned railway company, was forced to shut down for a week. This attack, however, was only one of many, as global statistics show that a cyberattack takes place every 11 seconds.

With October being Cybersecurity Awareness Month, organisations should use this opportunity to re-evaluate the safeguards they've implemented and also add new measures if their workforce is largely distributed. This article looks at five factors that businesses can implement to secure their workforce:

1. Clearly define security policies and procedures

When establishing policies and standards, companies must consider their cloud platforms, software development lifecycles, DevOps procedures and technologies, and compliance with regional regulations. Basic security hygiene alone is not sufficient at the enterprise level to protect against advanced cyberattacks.

When putting together policies, businesses should keep in mind the following:

- Consider current threats, compare them to industry standards, and devise a comprehensive security strategy.
- Publish transparent security policies and standards internally to assist internal stakeholders in making critical security decisions.
- Set goals, processes, and accountability to achieve the overall company's security policies and standards.

2. Train, equip, and reward

It is important to educate all employees on the evolving threat landscape. Businesses should educate all stakeholders about the many types of dangers - from phishing to ransomware to social engineering. Are your staff aware of these threats, the damaging results of such an attack, and trained to know what to do and whom to call in the event of an attack?

Businesses should provide basic security tools to their employees, such as password managers, multi-factor authentication, data backup, and behaviour threat analytics. Threat analytics, especially, can help warn users and administrators when an account is accessed from an unknown IP during odd hours. Also consider incentivising employees with a rewards program. For instance, internal cybersecurity and bug bounty initiatives at Zoho have aided immensely in educating and rewarding responsible staff.

3. Protect identities and access keys

Identity and key protection should be a primary priority for every cybersecurity team. It's critical to securely authenticate and authorise individuals, services, devices, and apps to ensure that only valid accounts/devices are able to access the company's data. For example, many businesses now use SSH keys and SSL certificates in the background to perform safe cryptographic operations.

When it comes to identity management, the beginning point is to implement tactics such as strong passwords, passwordless authentication, multi-factor authentication, role-based access, identity-based perimeters, and zero-trust access control strategies.

4. Secure the endpoints

Once an identity has been granted access, a user can gain access to numerous endpoints and applications owned by the company using the identity. In a hybrid environment, enterprise data is communicated over smartphones, IoT devices, BYOD, cloud servers, and more, and many companies still rely on traditional firewalls and VPNs to restrict access. Rather than relying on these legacy models, companies should adopt a least-privilege access strategy for users, applications, systems, and connected devices. It's important to provide only a minimum level of access based on job roles and responsibilities. This technique has the following important benefits:

- Cyberattack surface is reduced
- Better control on malware spread
- Increased efficiency in compliance and audits

5. Keep applications up to date

Unpatched systems and apps are some of the easiest targets for hackers. Whenever a new security patch is issued, attackers will attempt to exploit the flaw before the patch is applied in order to obtain access to corporate data. Thus, enterprises should take advantage of patch management and vulnerability management tools that offer immediate implementation. Other benefits include improved efficiency and simplified compliance, helping avoid unwarranted fines.

Businesses in South Africa are currently more interconnected than they have ever been. While this is a development that will help many industries thrive, it also implies that businesses must prioritise cybersecurity to ensure successful benefits realisation. The truth is that it's a matter of 'when,' not 'if,' your company will be targeted, and being prepared with a robust cybersecurity and resilience strategy is the greatest defence.

ABOUT ANDREW BOURNE

Andrew Bourne is Zoho's regional manager for the Africa region and is based in Cape Town, South Africa. He has more than 15 years of experience in sales and marketing and has spent the last five years focusing on the implementation and testing of various business technologies. He is very passionate about Zoho and has exceptional insight into the business and marketing world.

- What online privacy and security will look like in 2022 - 6 Jan 2022
- 5 cybersecurity tips to secure your workforce - 26 Oct 2021
- 5 important tips for your business website - 10 Mar 2021
- Why tech companies should open offices in small towns, villages - 10 Nov 2020
- 5 emerging SaaS trends for your business - 1 Sep 2020

View my profile and articles...