13 security controls for SMEs and cybercrime

SMEs are the perfect victims for cybercrime. Focused on getting their businesses off the ground, they are oblivious of the vast amounts of data they're accumulating, says Alain Tshal, district sales manager for Sub-Saharan Africa at F5 Networks.

Alain Tshal, district sales manager for Sub-Saharan Africa at F5 Networks.

The writing is on the wall: SMEs are prime targets for hackers. It is imperative that SMEs have robust measures in place to deter cybercriminals. Let's explore the top-recommended security controls for 2020 in order of urgency:

1. Use strong authentication to limit unauthorised access

Strong authentication is essential as access control attacks are prevalent and often the tip of the spear for most cyber-mayhem.

Multifactor authentication (MFA) is recommended, especially for any system that connects to high-value services and data stores. When MFA isn't feasible, strengthen the use of passwords.

Key tips include regularly checking passwords against a dictionary of easy-to-hack credentials, using long passwords and eliminating password hint mechanisms. All authentication systems should have a mechanism to detect and throttle floods of login attempts.

2. Practice regular monitoring and logging

Monitoring and logging are all about knowing what is going on in your environment. With a good logging and review regimen, it's possible to catch breach attempts in progress before real damage can occur. When reviewing logging capabilities, remember the goal is to be able to determine how an attacker got in and what they did.

3. Take inventory

Knowing what you have, where it is, what it talks to and how it is configured is the foundation for all risk decisions, both strategic and tactical. While there are plenty of automation tools available, it is important to ensure they are a precise fit with your specific business requirements.

4. Strategise and practice incident response

No affordable defence is going to keep all attackers at bay forever. Plan accordingly with a well-tested and detailed incident response plan. Incident response relies on strong inventory and logging practices, so make sure those are well-honed.

Each major threat should have response scenarios that include trigger definitions (when an incident occurs), activation plans (who and what jumps into action and when), intelligence collection (what logs and devices should be examined), containment (specific playbooks to activate additional controls), investigation (who analyses what and when), reporting (for legal and executive conversations), and recovery (of both data and system rebuilds).

5. Apply crucial patches

It's unreasonable to assume that the average enterprise is going to patch everything without shutting down all useful work. The highest priority is closing vulnerabilities with published, weaponised patches. Even unskilled attackers will pound your systems with these types of point-and-click attacks. Browsers and mail clients should also be kept up to date to safeguard against malware.

6. Enforce strict authorisation

Authorisation means forensically interrogating permissions associated with any credential set. Once someone is logged in, what can they do? This is where the 'principle of least privilege' should be used so that users can only perform tasks specific to them. A good middle ground is to implement role-based access and broadly lockdown authorised actions based on general job duties such as administrator, developer, office staff and remote user.

System administrators are frequently targeted by attackers due to their unrestrained access to resources Administrative usage should be partitioned to just the systems a given administrator is responsible for managing. The same goes for service accounts that run in the background.

7. Scan for vulnerabilities

Vulnerability scanning is useful for gaining a 'hacker's eye view' of your systems and is also a great way to double-check your inventory. Weekly vulnerability scans are advisable for both internal and external assets.

8. Detect and block malicious bot activity

It's getting harder to identify humans. Many bots are evident from previously observed, unique patterns that have been encoded into signatures. However, newer and more sophisticated bots require deeper analysis such as looking for irregular behaviour and illogical client configurations.

9. Conduct security awareness training

F5 Labs analysis notes that training employees to recognise phishing attempts can reduce their click-through rate on malicious emails, links and attachments from 33% to 13%. The key to effective training is to consider what decisions you want your users to make and what you can reasonably expect from them.

10. Use web application firewalls (WAF)

Web Application Firewalls (WAF) are essential for application protection. The technology offers a level of application-layer visibility and control that can help mitigate a wide range threats. Many WAFs also include the capability to inspect, validate and throttle API requests (the transfer of resources between connected applications).

11. Use SSL/TLS inspection

More and more malware and phishing sites are being buried within encrypted SSL/TLS sessions, often using legitimate certificates. This traffic needs to be decrypted, inspected, and sanitised.

12. Use antivirus solutions

Antivirus remains a powerful tool for detecting and stopping malware infections. It should always be configured to update its signatures without intervention and alert when it stops functioning.

13. Love your apps

Get to know and love your apps, wherever they are. Always make sure your controls are fit for purpose and running smoothly.