DR LAMEK RONOH, *Senior Lecturer/Dean, Rongo University*
LinkedIn/Website : linkedin.com/in/lamek-ronoh-929737140

Lamek is Senior Lecturer and current Dean at Rongo University with research focus in Cybersecurity, Data Science and Machine learning. Certified in Cyber security and skilled in vulnerability scanning, penetration testing, programming (C, C++, Python), Open-Source Intelligence (OSINT) and knowledgeable in industry standards and frameworks and skills of ensuring robust information security protocols and efficient service management practices.

TIP 1. ESTABLISH CONFIGURATION INVENTORY

A business entity to consider establishing a configuration management inventory that stipulates baselines standards that any hardware and software configurations changes must adhere to and recorded and not compliance to the security baseline will be flagged off and action taken. The baseline standards contain system specification configurations that are considered compliant and secure. Software updates, patches and hardware configurations are recorded and counter-checked against the established baselines to check for any anomaly

TIP 2. IOT ATTACK VECTORS: A NEW RISK TRAJECTORY

Watch your business entity(s) for new attack vectors that are likely to leverage weak security configurations that maybe inherent in common IoT devices such as routers, networked printers and other IoT devices. Protect your business from IoT threats by segregating network of IoT devices and implementing zero trust policy, sealing weak configurations, disabling unused features in IoT devices. Frequently monitor and flag off any suspicious activity.

TIP 3. THREE IMPORTANT ASSETS

Be wary of a unique threat landscape that targets business assets comprising of data, credentials and applications assets. Safeguard your credentials by implementing a robust access control to authenticate and authorise users. Protect your business data either at rest or at transit by use of robust encryption mechanisms and adoption of secure channels of communication and up to date digital certificates. Consider security trade-offs between in-house and off-the-shelf applications

TIP 4. PROTECT WHAT YOU VALUE

What are your business's irreplaceable valuables that you cannot afford to lose? Invest in protecting what you value most in your business by applying sufficient security measures that will allow transactions safely in the cyber space. Conduct a thorough business impact analysis to identify and classify to identify the critical business data and asses the degree of damage that critical business data will impact the business if compromised.

TIP 5. KERBEROS HIGHWAY

Business growth implies exponential expansion in technology infrastructure that also comes with its security challenges. To counter this, SMMEs should consider to implement Kerberos cyber security stateless authentication method which works by employing trusted third-party authentication to issue ticket mechanism that is time-stamped to ascertain the identity of a suer on an unsecured network. This way, passwords are not repetitively sent over the network; hence preventing the eavesdropping cyber security threats between business entities.

TIP 6. IMPLEMENT PRINCIPLE OF LEAST PRIVILEGE

Granting system users limited access to carry on their job functionalities not only minimises risks such as unintentional or intentional data leakage; but it also leads to reduction of attack vectors and surfaces that cyber criminals would otherwise take advantage of if the system is compromised by the user with full or escalated privileges. This way, business entities are able to maintain a secure computing environment and assure business continuity.

TIP 7. ACCESS CONTROL: WHICH ROUTE?

Comparatively, the ideal access control mechanism for SMMEs is Role-Based Access Control (RBAC) model which assigns permissions to roles rather than individual users. This mechanism aligns well with scalability, resource constrained and dynamism nature of SMMEs. With RBAC, proprietors of SMMEs will be able to manage their staff during hiring, onboarding and separation hence minimising potential security risks.

TIP 8. COMPREHENSIVE SECURITY POLICY

One overall ICT security policy is not good for a security minded business entity. Instead, SMMEs should develop separate, but related, ICT policies such as an Organisational ICT security policy whose aim is to create a secure computing environment in an organisation; Issue-based ICT security policy – which guides users on best practices and System -based ICT security policy which solely addresses the aspects of maintenance and configurations of systems.

TIP 9. INVEST AND LEVERAGE ON AI

Out of a tight budget, SMMEs should consider investing and deploying AI/ML cyber security solutions that not only leverage on security information and event management (SIEM) functionalities but also automatically detect security breaches such as zero-day vulnerabilities and perform auto-scanning for vulnerability detection. Continuous training of the model to remain up to date with emerging threats will be implemented

TIP 10. IMPLEMENT CIS CONTROLS

In the quest to improve their security readiness, SMMEs should adopt and deploy CIS (Center for Internet Security) controls that concentrate on specific business processes. This way, business entities are able to reduce emerging threats; and also get a platform to select and adopt an up to date security framework with tested and well-defined actionable activities that does not need resources or in-depth cyber security knowledge.