Adopting zero trust defence

AS we navigate the complexities of a digital era, the increasing frequency and intricacies of data breaches underscore the critical need for robust cybersecurity measures.

These incidents not only compromise the privacy of individuals but also pose a substantial threat to the integrity of our financial systems, communication networks and even the democratic processes, which are the foundation of our society.

From KPMG's perspective, the National Digital Identity (IDN) should not only function as a means of identification but also serve as a cornerstone for enhancing cybersecurity and fortifying Malaysia's digital infrastructure.

According to the Personal Data Protection Department, as of September 2023, there were 15 data breaches occurring every week in the country where at least five are personal data breaches. Among the notable data breaches were:

● Nov 28, 2022 - A database containing 487 million WhatsApp user mobile numbers, including 11.7mil belonging to Malaysians, was reportedly offered for sale on a hacking community forum.

● Dec 28, 2022 - Telekom Malaysia Bhd identified 250,248 Unifi Mobile customers affected by a data breach involving individuals as well as small and medium enterprises.

We believe the government needs to address some of the key challenges and implement better practices in rolling out the IDN by:

● Establishing a robust rules framework, encompassing national standards, trust frameworks, jurisdictional policies and legislation, particularly related to data privacy and consent. This is crucial in establishing accountability and oversight. Additionally, standards around data, Application Programming Interfaces (APIs) and interoperability should be set to facilitate seamless and secure integration, especially with the private sector.

ALVIN GAN

Head of Technology Consulting at KPMG in Malaysia

● While 90% of the government's services are already online, there is a plausibility of a disparate data and technology landscape as each agency has its own identifiers. It is vital that the government ensures the readiness of these technologies, including the data infrastructure to ensure a successful rollout to both the public and private sectors. Operationalisation upon establishing the rules framework is crucial and collaborations to establish detailed policy and procedures are important to ensure that operational challenges can be captured and addressed.

● Recognising the rakyat's concerns and fears regarding the IDN initiative, it is imperative that public engagements and awareness campaigns are carried out to educate them on the mechanics, safeguards as well as the benefits of the programme.

Implementing IDN is critical due to increasing digitilisation of the public and private sectors' services, coupled with rising customer expectations for seamless digital experiences across different industry verticals.

■ IDN can contribute to the advancement of financial inclusion in the country

IDN can play a pivotal role in establishing trust and security in transaction processes, particularly in the e-commerce space. It can act as a deterrent against fake accounts, enhance the e-KYC (electronic Know Your Customer) norms for customer verification as well as enable smooth deliveries and returns. This will build the rakyat's confidence in adopting online shopping and payments.

The initiative can also contribute to the advancement of financial inclusion in the country. Individuals, particularly those from lower socio-economic backgrounds, can be formally brought into the financial system. This can stimulate more digital transactions and contribute to informed policymaking through extensive data availability.

IDN will also streamline and enhance delivery of social welfare programmes and government subsidies. It supports secure and efficient verification of the identity and eligibility of the beneficiaries, which in turn can help reduce fraud and leakages. Its integration with the digital payment infrastructure will also enable direct transfers of subsidies, eliminating paperwork and delays in government processing.

Fostering better regional cooperation will also be easier with standardised frameworks that facilitate seamless cross-border authentication, easing the movement of people and labour as well as financial transactions. Thus cross-border IDN will play a pivotal role in advancing Asean's financial integration agenda.

With global digital ID adoption set to surge by over 50% from 4.2 billion users in 2022 to 6.5 billion by 2026, its growing significance in accessing government services is evident. For example, Estonia has successfully implemented a digital ID system whereby nearly all government services are available online. This not only enhances ease of access for its 1.3 million citizens but enables it to save 2% of its GDP value annually.

Delaying IDN's implementation risks Malaysia missing out on this global trend, impacting citizen engagement as well as economic and administrative efficiency. Addressing the nation's data and technology infrastructure hygiene is of utmost importance, as data integrity and reconciliation across government databases are crucial to enable seamless and accurate authentication whilst maintaining privacy.

This is where the guiding principle of "assume nothing, verify everything" will be useful. If the IDN initiative is to become a reality, KPMG strongly recommends that all stakeholders, particularly the rakyat, embrace the zero-trust principle.

This approach puts user identity, access management and data at the core of cybersecurity. It is an evolutionary cybersecurity model in response to the ever-expanding threat landscape. In a zero-trust model, no one, whether inside or outside the network, is automatically trusted.

The government must assure the rakyat that robust governance and controls will be instituted to safeguard their rights. A specific strategy for outsourcing services needs to be instituted, particularly if third parties are involved.

This includes establishing appropriate governance arrangements and enforcing more stringent cybersecurity measures. A proactive approach would address concerns and instil public confidence with regard to the responsible handling of personal data.