SCIENCE & TECHNOLOGY

Indonesia's Vulnerable Cybersecurity Puts SIPD at Risk

The National Data Center (PDN) ransomware attack in Indonesia at 20th June has had a detrimental impact on various ministries/institutions, stalling the business process.

BY **MUHAMMAD RAFI BAKRI** SEPTEMBER 13, 2024

Authors: Muhammad Rafi Bakri and Rifky Pratama Wicaksono*

The National Data Center (PDN) ransomware attack in Indonesia at 20th June has had a detrimental impact on various ministries/institutions, stalling the business process. One consequence of this incident is that passport checks at airports are becoming more difficult due to data issues. Then, about 800 thousand student data receiving educational assistance from the Ministry of Education is also impacted, causing recipient students to bind their data back. In total, this attack hampered 210 central and regional government databases.

If regarded positively, this incident can warn the government to be more cautious about cybersecurity from data. The data kept digitally is highly vulnerable to theft and potentially criminal usage, such as selling personal information. It can contain personal information that can be used by fraudsters so that the potential loss will be broader.

In 2020, the Ministry of Home Affairs (MoHA) established the Regional Government Information System (SIPD). SIPD evolves into a database that provides interconnected information on development and finances for local governments, utilizing PDN facilities for data backup. Besides, SIPD has transformed from a monolithic to a microservices base, resulting in enhanced functionality.

Without aiming to underestimate SIPD's performance, it has the potential to experience the same leakage as PDN. This argument is not without merit since it is based on audit results on the MoHA conducted by the Audit Board of Indonesia (BPK) that assess the effectiveness of the SIPD itself. The audit findings revealed five critical issues, including SIPD's cybersecurity vulnerability.

According to Audit Report Number 3/LHP/XVIII/2/2024, BPK discovered inadequate information security management in SIPD. For starters, the MoHA lacks the guts to handle database security on its own. Until now, the MoHA has granted developers full-access to SIPD that are being created or deployed. Moreover, the Ministry did not issue a Non-Disclosure Agreement (NDA) or engage with developers, ensuring that no fraud occurred by the developer, either purposefully or accidentally.

Furthermore, The MoHA might repeat what the PDN has happened because data backups have not been segregated from live data locations. This is extremely risky if the location of live data encounters a force majeure event, which could stop the entire SIPD system. This problem may be aggravated because the BPK discovered that SIPD's Disaster Recovery Center (DRC) is unsuitable. When the DRC of the database is inadequate, it is clear that the cost and time required to restore the system to its optimal state during the force majeure will be highly expensive.

To avoid the same fate as the PDN, what steps must the MoHA take?

Unfortunately, modifications to the digitalization of government are not founded on a digital mindset, resulting in no significant shift in business operations compared to before the implementation of SIPD. The government just changes the technique, not the transformation, so that the usage of SIPD causes more disturbance and increases expenses. The SIPD also appears to be in a hurry without considering benchmarks, such as the Ministry of Finance that established the SAKTI application that many central government institutions have utilized.

Comprehensive norms, standard, and procedures related to information security management system are the most fundamental aspect to be considered. The SIPD task force which involves multiple divisions, including regional governments across Indonesia as stakeholders and users, should establish cross-sectional security protocols to ensure a unified and robust defence against potential threats. This includes stardizing data protection procedures across all departments, and encouraging collaboration to solve security issues proactively.

In order to manifest a sustainable cybersecurity on SIPD, MoHA must design a cybersecurity roadmap by continuously assessing both internal and external information security issues. The ministry should perform systematic risk management process by identifying all possible risks, calculating the impact, appraising the SIPD's pre-existing condition, and mitigating them through certain measures whilst surveiling the cycles.

To maintain the resilience and availability of essential data, MoHA must implement robust data backup regulations. This includes implementing frequent and thorough backup methods, developing plans to guarantee continuous access to data and information, and putting together effective recovery systems. As a benchmark, Thailand has at least 16 identical systems operating simultaneously, so the e-government system will be very stable and resistant to cyber-attacks. This made Thailand's e-government score soar to 53rd place, higher than Indonesia's.

Additionally, DRC also necessary to countermeasures the service issues caused by software functionality, human error, anticipate unpredictable force majeures, and frequently inform the taken recovery procedures to the public. Thailand's system is hosted by 4 cloud provider consortiums across 4 separate geographic zones. Furthermore, one server was transferred overseas to improve DRC efficiency.

It is also important to optimize the role of cybersecurity incident response team dedicated to tackle information security incident in accordance with the regulation quickly and effectively, also to reduce the probability of cyber-attack to SIPD. To do this, collaborative move with the National Cyber and Crypto Agency (BSSN) in the field of cyber intelligence, defence, and security, is not enough.

MoHA should also invite cybersecurity consultants to conduct training and workshop programs, allow employees to earn certifications like Certified Ethical Hackers, and benchmark against countries with successful cybersecurity systems to learn and adopt best practices. These methods would prepare MoHA staff to handle SIPD cybersecurity threats. Singapore, the world's third-best e-government, educates its personnel on handling cyberattacks. They plan to teach non-cyber workers in cyber defence to improve cybersecurity in Singapore. Singaporean women can also take 10,000 cybersecurity courses.

MoHA faces significant hurdles in protecting SIPD against cyber threats. Cyber-attacks are inevitable, as every country has experienced them. However, many factors that trigger a weak defense system can be addressed with preventive measures to eradicate them and not hinder them if a cyber-attack on the SIPD occurs, preventing PDN Chapter 2 happened.

**Rifky Pratama Wicaksono is a policy technical reviewer at The Audit Board of Indonesia, while Muhammad Rafi Bakri is a data and finance analyst at The Audit Board of Indonesia.*