Title: Advisory on Data Breach Prevention

Introduction

National Cyber Security Agency (NACSA) is aware of the recent incidents of data breaches involving personal data of citizens in this region.

Impact

Information leakage, information loss, service disruption and integrity of information compromised.

Brief Description

For the past several months, NACSA has seen multiple data breach incidents involving citizen personal data in Malaysia as well as within the South East Asia region, with the most recent case happened in Singapore which affected more than 1.5 million personal data including health details of Singapore Prime Minister.

While there's no party has claim responsibility for any of the previous incidents, the Cyber Security Agency of Singapore (CSA) and the Integrated Health Information System (IHIS) have revealed that recent attack on SingHealth is a deliberate, targeted and well-planned cyberattack that could very well have been a state-sponsored attack, which specifically and repeatedly target the details of Singapore Prime Minister personal and outpatient medical data.

Therefore, in the wake of this event, organisations are urged to take the necessary actions to protect clients' and stakeholders' personal data accordingly and adhere to Personal Data Protection Act (PDPA) 2010 and/or Official Secret Act (OSA). Organisations are reminded to always be vigilant in order to avoid from becoming a victim of these incidents.

System Affected

All operating systems, web servers, databases & online services.

Recommendation

Organisations and Security Operation Centres (SOCs) are required to take the following actions:

1. Perform regular security test on your application systems to check for vulnerabilities and loopholes;
2. Update your critical assets with the latest security patches and updates;
3. Warn your users not to open or click on unsolicited mails and links with/without attachments;
4. Ensure that anti-virus/anti-malware signatures are up to date and functioning;
5. Disable FTP services where unnecessary;
6. Block or restrict access to every port such as port 3389(RDP), port 5900 (VNC) and port 22 (SSH) and services except for those that should be publicly available;
7. Review your user credentials list for any new additional unknown user;
8. Encrypt your database;
9. Monitor your environment closely for any anomalies;
10. Check whether your organisation's credentials been exposed in pastebin;
11. If you suspected that your servers have been compromised, conduct a proper incident handling and escalation; and
12. Report immediately to NACSA if your organisation fall victim to a data breach.