silverlake
SYMMETRY AT WORK

masterSAM

Silverlake MasterSAM Threats in Digital Governments

Threats in Digital Governments

The rapid speed of digitisation and technological improvements have increasingly threatened data security and privacy. With rising number of businesses across the globe going digital, the data security and privacy threats have increased considerably and stealthily targeting major institutions and wreaking havoc over the last few years. Zettabytes of cardinal information and billions of dollars are at risk. No one can be said to be spared - be it small enterprises or government institutions of large-scale.

Despite this systemic impact, according to a recent A.T. Kearney's research, ASEAN countries in general are apparently under-spending on cybersecurity. Among these countries, however, Singapore and Malaysia are one of the few ASEAN countries to have placed cybersecurity as one of their primary digital transformation agenda. Being one of the Asia Pacific region's major technology and financial hub, highly-networked Singapore is more susceptible to cybercrime attempts. Moreover, with its move to become digitised, it is even easier for hackers to target Singapore.

In 2017, the Deputy Prime Minister of Malaysia, had announced a new law that aimed specifically at this very purpose of protecting its citizens and ensuring national security. Enforcement agencies such as National Cyber Security Agency (NCSA) have to solely depend on the existing legislation, such as the Communication and Multimedia Act 1998, the Defamation Act 1957 and the Sedition Act 1948, to combat cyber threats. Such sole dependence on these few legislative practices may seem inadequate to protect citizens and organisations from cyber threats as it is a tall order to keep pace with the rapid advancement of modern technology and the risks it brings along.

In early 2018, the World Economic Forum (WEF) announced a new Global Centre for Cybersecurity in an effort to safeguard the world from hackers and protect against rogue nation-states. The goal of the centre is to create a safe and secure global cyberspace, allowing collaboration between governments, businesses, experts, and law enforcement agencies for protection against cybersecurity attacks.

Who might be attacking you?

While we see the headlines on the cyber threats attacking even the largest legislative governments and numerous legislative bodies taking active steps, it is also important to understand how they all begin - who the culprits are.
A brief overview of the various parties planning to attack the sensitive IT environments is listed below:

1. **Cyber criminals** who want to make money through fraud or from sale of valuable or national sensitive information.
2. **Industrial/International competitors** and **foreign intelligence services**, who want to gain an economic advantage for their own companies or countries.
3. **Thrill-seeking** hackers who simply enjoy interfering with national security systems and data.
4. **Hacktivists** who wish to attack companies for political or ideological motives.
5. **Insider attacks** through **employees of the government agencies** or those who have legitimate access, either by accidental or intentional abuse.

Impact of Cyber Security Threats on Government Institutions

Cyber security is not only a challenge. It is a huge hindrance to a government's initiative in **digital transformation**.

When hackers gain unauthorised access to systems or engage in an improper use of computing resources or install malicious software, the impact on the government IT infrastructure systems could be phenomenal. Impact includes but not limited to loss of personal or highly sensitive information, disruption or destruction to the critical infrastructure and devastating damages to national and economic security. Much of these damages are irreversible and it may be a tall order to salvage such a situation, when the agency does not have the right tools and processes to safeguard its cyber space.

According to a report shared by the Singapore Government, the nation had about 16 major / minor cyber-attacks from April 2015 to June 2016. 16 attempts in a year imply almost more than 1 attempt in a month. With Singapore businesses and government institutions becoming increasingly aware of the threat of cyber-attacks, these numbers are indeed worrying.

Threats in Digital Governments

1. **National Security at peril** - when public sector information is hacked and stolen
2. **Citizen's trust takes a dip**

It is integral to have the right protective and preventive mechanisms in place. As per the National Cyber Security Policy, the Malaysian Government has listed 10 important sectors in Malaysia known as the Critical National Information Infrastructure ("CNII") which are required to be protected to a level that is apt for the risks faced.
The CNII sectors primarily are:

- National Defence and Security
- Banking and Finance
- Information and Communications
- Energy
- Transportation
- Water
- Healthcare services
- Emergency Services
- Food and Agriculture
- Government

It is an interesting fact that not only must the government protect its own IT infrastructure, but also devise and implement plans and mandates to secure all other industries that serve its citizens.

The steps towards combating Cyber Security Threats

The key to a successful protection programme necessitates effective governance and coordination. The preventive mechanisms chosen and implemented should enforce trust in the system and in the minds of the citizens. The processes implemented should bring accountability and transparency in the IT enterprise security management. Cyber Security enforcement must be made everyone's job so as to build a culture of cyber security awareness and embed it as an organisational mindset.

The government body needs to identify the right vendor in the cyberspace who have a trusted reputation in the business - a reputation of introducing a holistic approach and easy deployment to resolve and bridge the gaps in the cyber security.

What does "Privilege" have to do with threats facing the governments?

The least-privilege approach has gained a lot of momentum and popularity in the recent past due to increased number of cases of data leaks and breaches. Also, it is remarkable to note that insider attacks and abuse of privilege were discovered by the 2014 Verizon Data Breach Investigations Report as one of the nine basic patterns of activity in the past decade that have resulted in confirmed data breaches. The most effective approach therefore would be to restrict access privileges through stringent policies and technology restrictions - such that the privilege is offered only as per the need arising.

Why Silverlake MasterSAM?

Silverlake MasterSAM, one of the premier APAC Compliance Solutions Providers, is a technology leader specialising in comprehensive and credible suite of Privileged Access Management security solutions. Established in 2004 and acquired by the Silverlake Group in 2015, Silverlake MasterSAM strives to protect and manage the most sensitive IT enterprise business platforms from a complete life-cycle perspective. With a strong belief that "A great product comes from real users", we at Silverlake MasterSAM, keenly listen to understand core problem areas of our customers. Augmenting this customer-centric approach is our strong innovative spirit that places elaborate focus on research and development in the privileged access management domain.

Threats in Digital Governments

The attackers would initially spend large amount of time researching a list of potential targets, gathering information about the organisation's structure, clients, etc. Next, they would start hunting for system admins where internal networks are compromised. When an employee or third-party accidentally installs malware, cyber perimeters are breached. The hacker then observes the system and uses their legitimate VPN login to look for their opening. Once hackers gain a foothold by passing-the-hash, they execute lateral movement under the guise of authorised privileged users. Privileged accounts are often targeted as they are the direct pathways to access highly-guarded infrastructure containing proprietary information. Examples of privileged accounts include system accounts, administrative accounts, shared accounts and service/application accounts. At last, the hacker would be able to obtain the keys to the crown jewels and locate desired data. The system is then compromised. However, such threats could have also brewed from within known as "Insider Threat" caused by inadvertent employee behaviour.

Use Cases

USE CASE 1: Managing privileged access

Objective: To control and restrict administrator access to the most sensitive data sources in the government agencies

How Silverlake MasterSAM PAM solution helps:

Administrator to login to Silverlake MasterSAM platform with daily privileged access. Whenever a higher privileged credential is needed to perform specific task, administrator will go through approval request workflow to submit a ticket. When the request is approved, administrator will be able to access the system with higher rights going through Silverlake MasterSAM. In short, only authorised users have access to privileged accounts. Access can be defined for each target user, third party, or sub-contractor (including changing and revoking access permissions as needed). Users will also be prevented from elevating their own permissions.

USE CASE 2: Surveillance, Review and Audit

Objective: To record, play back, review and alert on user activities that can happen in the IT enterprise platform of the government body

How Silverlake MasterSAM PAM solution helps:

With PAM solution deployed, all activity on privileged accounts is monitored and tracked (including what information was accessed and what was done during the session). All access sessions to target system through Silverlake MasterSAM can be recorded in text and in video format. Keywords appearing in these captured screens can also be traced and a rule-based alert system can be set up. Reviewer will be able to play back user access sessions to check on activities are / was being performed. Live monitoring also ensures that no violation can ever happen and all sensitive data will be secured.

Based on this, the government body is also able to effectively extract provisional reports that include statistics, behavioural analysis, etc on each user activity. It paves way for a smooth unalterable audit trial and help me key government regulations.

Use Cases

USE CASE 3: Password Retrieval

Objective: To safekeep and monitor password usage for key user platforms on the government websites, internal records.

How Silverlake MasterSAM PAM solution helps:

Passwords are protected in a vault that can allow administrators to easily and confidentially hide, reveal, generate, and change passwords. All privileged account passwords will be checked in and safely stored in Silverlake MasterSAM password vault. Whenever a request is needed to release the password, requestor will need to submit for approval in order to retrieve the password. All the usage of the password will be logged for audit purposes in Silverlake MasterSAM.

Users are prevented from elevating their own permissions

Organisations receive provisional reports that include statistics and behavioural analysis based on user activity

Enterprises can meet IT compliance with an unalterable audit trail

USE CASE 4: Meeting Compliance Standards

Objective: To meet the mandatory compliance regulations (such as ISO 27001 and IM8)

How Silverlake MasterSAM PAM solution helps:

The team at Silverlake MasterSAM who have carefully assessed the requirements of these regulations are well-versed to prepare the government body to conveniently meet the mandatory requirements stipulated by the standards.

Contact us

For more details on how Silverlake MasterSAM can assist you in deploying Privileged Access Management in your organisation, write to us at mastersam.info@silverlakeaxis.com

We relentlessly pursue innovation to ensure our valued customers and partners benefit from the most practical and trusted solutions for all their complex cyber security concerns. Silverlake MasterSAM, headquartered in Singapore, has an expansive presence in the region with offices in Malaysia, India, Vietnam, Philippines, Dubai, Australia and Slovakia.