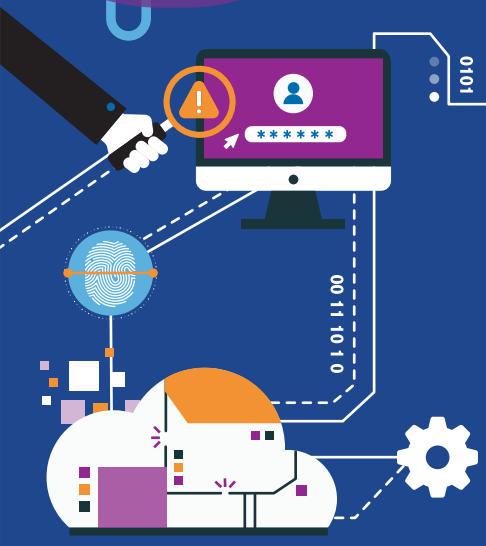
pdpc
PERSONAL DATA PROTECTION COMMISSION SINGAPORE

GOOD PRACTICES TO SECURE PERSONAL DATA IN THE CLOUD PLATFORM



Increasing digitalisation has spurred more organisations to adopt cloud services and platforms. With the security features in-built by the cloud service providers (CSPs), cloud services and platforms are generally more secure than on-premises implementation. However, data breaches can still occur when organisations do not comply with good practices and security policies in managing their cloud assets.

We have compiled these basic good practices to avoid common types of cloud-related data breaches. Organisations are encouraged to start implementing these to protect personal data in the cloud.

Misconfiguration of Cloud Platforms

CASE EXAMPLES

- **Organisation A** wrongly configured cloud storage as publicly accessible and it contained personal data. As a result, the exposed cloud storage led to the disclosure of personal data.
- As part of a data migration exercise, **Organisation B** negligently breached security by configuring the setting of an exposed port to "public" without any security restriction on the cloud. This has led to the threat actor gaining unauthorised access to the cloud storage containing personal data.

IMPLEMENT ROBUST CONTROL TO CLOUD RESOURCES SUCH AS:

I. Whitelist or allowlist IP address that are allowed access to cloud resources.
II. Configure "private" access for cloud resources by default.
III. Periodically audit cloud configurations and security controls to ensure compliance to the organisation's security policy.

Malware and Phishing

CASE EXAMPLE

- The employee of a domain provider was tricked through social engineering to transfer control of its domain hosting account belonging to **Organisation C**, to an external actor. With the control, the external actor redirected all of Organisation C's cloud-based email traffic to its own email servers. The external actor gained information to reset email passwords and successfully changed the password for a DevOps account which had access to the cloud storage database and stole sensitive personal data.

PROTECT YOUR CLOUD INFRASTRUCTURE AGAINST MALWARE AND PHISHING THROUGH:

I. Turn on advanced protection services such as Microsoft 365 advanced protection and Google Protection service for cloud-based email server to protect incoming mail.
II. Disable email auto-forwarding feature by default for cloud-based email server especially if the email accounts are handling sensitive personal data.
III. Use a one-time password ("**OTP**") or 2-Factor Authentication ("**2FA**") / Multi-Factor Authentication ("**MFA**") for securing administrator account(s) whose job function entails regular access to sensitive personal data or large volumes of personal data.

Compromise of Cloud Access Keys

CASE EXAMPLES

- All the developers in **Organisation D** were given full access privileges to access keys to cloud resources without any security restrictions. As there were no defined proper user role or groups to manage access keys to critical cloud resources, the threat actor used credential stuffing to obtain unauthorised access to the database hosted on a public cloud.
- Both former & current employees of **Organisation E** had access to old access keys left in the Github repository which had not been rotated or changed. With these compromised access keys obtained through credential stuffing, the threat actor was able to gain admin privileges and unauthorised access to cloud storage to retrieve sensitive data.
- **Organisation F's** employees often communicated and shared access keys via email in plain text, the threat actor managed to obtain the compromised access keys via phishing email to gain unauthorised access to cloud storage and personal data
- **Organisation G** had embedded access keys within an obsolete application source code on Github repository. A security breach occurred because the organisation had forgotten to remove the obsolete application source code that contain the access keys which was easily accessible by threat actors from the internet.

ADOPT GOOD CLOUD SECURITY PRACTICES AS FOLLOWS:

I. Limit the access privileges of cloud access keys (access key id plus secret access keys) based on user roles/functions, i.e. generate these keys using accounts with the least privileges needed for the user roles/functions, instead of using root accounts.

II. Do not embed cloud access keys (access key id plus secret access key) directly into source codes.

III. Use standard key management solutions to store and manage critical keys.

IV. Conduct periodic review on deletion and rotation of critical keys.

V. Conduct scans for cloud access keys that might be committed in shared repositories such as install a tool called "shhgit" to detect possible secret keys being committed to GitHub repositories.

For other good practices that you can adopt to safeguard against common data breaches, please refer to PDPC's **Guide to Data Protection by Design for ICT Systems** and **How to Guard Against Common Types of Data Breaches**.

For security configurations on cloud services and platforms, you may refer to specific CSP recommendations by Center for Internet Security at **CIS Benchmarks for securing cloud services.** Organisations can also consider using various useful tools provided by the different CSPs such as configuration scanning or sensitive data scanning services, to better secure their cloud assets. For a quickstart secure configuration guide for Google Workspace and Microsoft 365 Office, please refer to PDPC's **DPE Configuration Guide**.

Supported by
INFOCOMM MEDIA DEVELOPMENT AUTHORITY

In support of
SG:DIGITAL

In consultation with
Alibaba Cloud • Amazon Web Services • Google Cloud • Microsoft Operations Pte Ltd • Seagate