

Data Security

ความปลอดภัยของข้อมูล หรือ Data Security เป็นมาตรการรักษาความปลอดภัยของข้อมูลตามมาตรฐานสากลหรือตามที่กฎหมายกำหนด จัดทำขึ้นเพื่อคุ้มครองข้อมูลส่วนบุคคลโดยใช้วิธีการและเทคนิคต่างๆ เพื่อรับรองความเป็นส่วนตัวของข้อมูล ตัวอย่างของมาตรการ เช่น การให้สิทธิในการเข้าถึงเฉพาะผู้ที่มีสิทธิ์เข้าถึงเท่านั้น และป้องกันไม่ให้บุคคลที่สามเข้าถึงข้อมูลโดยที่ไม่ได้รับอนุญาต

Data Security Strategy in AWS

1) Data Security Lifecycle

- CREATE:** ขั้นตอนการสร้างหรือการรับข้อมูล รวมถึงการปรับเปลี่ยนหรืออัปเดตเนื้อหาที่มีอยู่ สามารถเกิดขึ้นได้ภายในองค์กร (on-premise) หรือบนระบบคลาวด์โดยตรง ขั้นตอนนี้เหมาะสำหรับการจัดประเภทข้อมูลตามความละเอียดอ่อนและความสำคัญต่อองค์กร
- STORE:** ขั้นตอนนี้มักเกิดขึ้นเกือบพร้อมกันกับขั้นตอนการ CREATE เป็นการนำข้อมูลไปเก็บไว้ในคลังเก็บข้อมูล (Storage Repository) เช่น Data Warehouse, Data Lake, Data Lakehouse เจ้าต่างๆ หรือบน Cloud ของ AWS เช่น S3, EBS, Redshift ซึ่งข้อมูลเหล่านี้ควรได้รับการป้องกันตามระดับการจัดประเภทที่กำหนดไว้
- USE:** ขั้นตอนการเรียกดู ประมวลผล นำข้อมูลไปใช้ในกิจกรรมต่างๆ เป็นขั้นตอนที่ข้อมูลมีความเสี่ยงมากที่สุด เนื่องจากอาจมีการโอนย้ายข้อมูลไปยังที่ที่ไม่ได้รับการรักษาความปลอดภัยเพียงพอ
- SHARE:** ขั้นตอนการให้ผู้อื่นเข้าถึงข้อมูล อาจเป็นการแบ่งปันระหว่างผู้ใช้ภายในองค์กร ลูกค้า หรือพันธมิตรต่างๆ เมื่อมีการแบ่งปันข้อมูล องค์กรจะไม่สามารถควบคุมข้อมูลนั้นได้อีกต่อไป
- ARCHIVE:** ขั้นตอนการนำข้อมูลที่ไม่ได้ใช้งานอย่างสม่ำเสมอ เข้าสู่การเก็บรักษาข้อมูลระยะยาว (long term storage) ข้อมูลเหล่านี้ยังคงต้องได้รับการป้องกันตามระดับการจัดประเภท ซึ่งองค์กรอาจต้องพิจารณาความคุ้มค่าระหว่างค่าใช้จ่ายกับความพร้อมใช้งานของข้อมูล และข้อกำหนดทางกฎหมาย
- DESTROY:** ขั้นตอนการลบ/กำจัด/ทำลายข้อมูลอย่างถูกต้อง ขั้นตอนนี้ต้องมีการพิจารณาเป็นพิเศษขึ้นอยู่กับประเภทของระบบคลาวด์ที่ใช้งาน



2) Data Classification

- ✚ การจัดหมวดหมู่และติดตามข้อมูลในคลาวด์ มีความสำคัญต่อองค์กรต่างๆ ช่วยให้สามารถจัดการข้อมูล ปกป้องข้อมูล และปฏิบัติตามกฎระเบียบได้อย่างมีประสิทธิภาพ
- ✚ Amazon Macie ใช้ Machine Learning ในการระบุข้อมูลสำคัญ โดยการจัดเตรียมแดชบอร์ดและเครื่องมือแจ้งเตือนให้กับองค์กร ซึ่งจะช่วยให้มองเห็นภาพรวมและเข้าใจได้ง่ายขึ้นว่ามีการเข้าถึงหรือเคลื่อนย้ายข้อมูลเหล่านี้อย่างไร
- ✚ Amazon Macie วิเคราะห์ข้อมูลความปลอดภัยบนระบบคลาวด์ สามารถส่งข้อมูลไปยัง Amazon CloudWatch เพื่อตรวจสอบและวิเคราะห์เหตุการณ์ และ AWS Security Hub เพื่อจัดการความปลอดภัยแบบรวมศูนย์บนระบบคลาวด์ได้

3) Encryption

- ✚ สำหรับข้อมูลที่จัดเก็บอยู่ในระบบคลาวด์ (Data at rest) องค์กรมีวิธีการเข้ารหัสหลายประเภทที่สำคัญที่ต้องพิจารณาดังนี้
 - การเข้ารหัสไฟล์/โฟลเดอร์: วิธีนี้เป็นการเข้ารหัสข้อมูลที่ระดับไฟล์หรือโฟลเดอร์ โดยทำให้ข้อมูลทั้งหมดในไฟล์หรือโฟลเดอร์ถูกเข้ารหัส และต้องใช้กุญแจ (Secret key, Public key, Private key) เพื่อถอดรหัสข้อมูลเมื่อต้องการเข้าถึงข้อมูล
 - การเข้ารหัสดีสก์ทั้งหมดสำหรับไดรฟ์ข้อมูลเวิร์คโหนดบนคลาวด์: วิธีนี้ใช้ในการเข้ารหัสข้อมูลทั้งหมดในดีสก์หรือโปรแกรมบริการเก็บข้อมูลแบบเต็มรูปแบบ โดยทำให้ข้อมูลทั้งหมดบนดีสก์ถูกเข้ารหัส และต้องใช้กุญแจเพื่อถอดรหัสข้อมูลเมื่อต้องการเข้าถึงข้อมูล
 - การเข้ารหัสเฉพาะทาง (ฐานข้อมูล, อีเมล): วิธีนี้เน้นการเข้ารหัสข้อมูลที่มีความสำคัญเฉพาะเจาะจง เช่น ฐานข้อมูลหรืออีเมล ซึ่งช่วยให้ข้อมูลที่มีความลับมีการป้องกันเพิ่มเติม
 - การเข้ารหัสข้อมูลเก็บข้อมูลในรูปแบบคลาวด์: วิธีนี้เป็นการเข้ารหัสข้อมูลโดยตรงในระดับการจัดเก็บข้อมูลของคลาวด์ เช่น Amazon S3 ทำให้ข้อมูลถูกเข้ารหัสขณะที่จัดเก็บ และต้องใช้กุญแจเพื่อถอดรหัสข้อมูลเมื่อต้องการเข้าถึงข้อมูล
- ✚ Amazon ทำให้การเข้ารหัสข้อมูลแบบเว็บไซต์ต่อเว็บไซต์เป็นเรื่องง่าย (Data in transit) ด้วยการเชื่อมต่อ IPSec VPN ซึ่งเป็นซอฟต์แวร์ VPN ที่ใช้โปรโตคอล IPSec เพื่อสร้างช่องสัญญาณที่เข้ารหัสบนอินเทอร์เน็ต มีการเข้ารหัสแบบ End-to-End ซึ่งหมายความว่าข้อมูลจะถูกเข้ารหัสที่คอมพิวเตอร์ของผู้ใช้ และถอดรหัสที่ Virtual Private Gateway (VPG) บน Virtual Private Cloud (VPC) ของลูกค้า
- ✚ AWS Key Management Service (KMS) เป็นบริการที่ให้บริการเกี่ยวกับการจัดเก็บและการบริหารจัดการกุญแจเข้ารหัสที่แข็งแกร่ง
 - ทุกรูปแบบของการจัดเก็บข้อมูลใน AWS สามารถรวมเข้ากับ AWS KMS ได้โดยตรง ซึ่งหมายความว่าลูกค้าสามารถใช้ KMS เพื่อเข้ารหัสและถอดรหัสข้อมูลที่จัดเก็บใน S3, EBS, Redshift, และบริการอื่นๆ ใน AWS ได้

- ✚ AWS CloudHSM เป็นเครื่องมือที่ให้บริการในรูปแบบของ Hardware Security Module (HSM) ที่ครอบคลุมครบวงจร ช่วยให้ลูกค้าสามารถสร้างและใช้งานกุญแจเพื่อเข้ารหัสข้อมูล บนฮาร์ดแวร์ที่มีความปลอดภัยสูง ซึ่งผ่านการตรวจสอบตามมาตรฐาน FIPS 140-2 ระดับ 3

4) Data Loss Prevention (DLP)

- ✚ การป้องกันการสูญหายของข้อมูล (Data Loss Prevention) ถือเป็นอีกหนึ่งอุปสรรคที่ท้าทายสำหรับองค์กรหลายๆ แห่ง ในการนำมาปรับใช้ในบนคลาวด์
- ✚ Amazon Macie ช่วยในการป้องกันการสูญหายข้อมูลในคลาวด์โดยใช้ Machine Learning เพื่อระบุและป้องกันข้อมูลสำคัญ รวมถึงการตรวจจับพฤติกรรมที่ไม่ปกติ และสร้างการแจ้งเตือนให้ผู้ดูแลระบบทราบ

5) Monitoring

- ✚ การติดตามการเข้าถึงข้อมูลของผู้ใช้เป็นสิ่งจำเป็นสำหรับองค์กรทุกประเภท การเลือกเครื่องมือที่เหมาะสมและปฏิบัติตาม Best Practices จะช่วยปกป้องและลดความเสี่ยงที่มีต่อข้อมูลของลูกค้าได้
- ✚ Amazon GuardDuty เป็นบริการตรวจจับภัยคุกคามแบบต่อเนื่องโดยอัตโนมัติ ซึ่งมีการตรวจสอบกิจกรรมหรือพฤติกรรมที่อาจเป็นอันตราย เพื่อป้องกันการโจมตีบนบัญชี AWS อย่างมีประสิทธิภาพ

Security Control Changes


- ✚ ข้อตกลงระบบการบริการ (SLAs) ของผู้ให้บริการคลาวด์ และความพร้อมใช้งาน/ความทนทานของข้อมูลเป็นส่วนหนึ่งของกลยุทธ์ในการรับผิดชอบร่วมกัน รวมถึงการรักษาความปลอดภัยของข้อมูลนั้นมีความสำคัญเป็นอย่างมาก ผู้ใช้งาน Cloud มีหน้าที่ประเมินความต้องการของตนเองและเลือกบริการ Cloud ที่ตรงตาม SLA ที่ต้องการ
- ✚ เส้นทางการขนส่งข้อมูลบางอย่างมีความสำคัญอย่างยิ่งต่อความปลอดภัย ผู้ใช้งาน Cloud มีหน้าที่เลือกใช้โปรโตคอลการเข้ารหัสข้อมูลที่เหมาะสม เช่น HTTPS
- ✚ การใช้ระบบควบคุมความปลอดภัยข้อมูลบนคลาวด์เป็นข้อกำหนดที่สำคัญ ผู้ใช้งาน Cloud ควรศึกษาและใช้ประโยชน์จากระบบควบคุมเหล่านี้ เช่น การจัดการสิทธิ์เข้าถึงข้อมูล
- ✚ BYOK ช่วยให้ลูกค้าสามารถควบคุมกุญแจเข้ารหัสได้ในระดับหนึ่ง คือ สามารถสร้างและบริหารจัดการกุญแจเข้ารหัสก่อนที่จะส่งเข้าไปเก็บไว้บน Cloud ได้ หลังจากนั้นจะเป็นหน้าที่ของผู้ให้บริการระบบ Cloud ในการจัดการกุญแจเข้ารหัสเหล่านั้น

Example of Data Security in AWS service

1) S3 Security


 การเข้าถึงข้อมูล (Data access):

- IAM policies: ควบคุมการเข้าถึงโดยใช้ IAM policies ซึ่งสามารถกำหนดสิทธิ์การเข้าถึงข้อมูลตามผู้ใช้ (User)/กลุ่มผู้ใช้ (Group)/บทบาท (role-based) ได้
- Bucket policies: policies ที่ปรับใช้กับ Bucket แต่ละอัน และไม่มีผลกับ Bucket ใดๆ นอกเหนือจาก Bucket นั้น
- ACLs (Access Control Lists): ควบคุมการเข้าถึงข้อมูลที่เฉพาะเจาะจงแต่ละรายการภายใน Bucket และกำหนดสิทธิ์การเข้าถึงข้อมูลสำหรับผู้ใช้/กลุ่มผู้ใช้
- Query string authentication: เป็นวิธีการเข้าถึงข้อมูลแบบ REST API (เป็นอินเทอร์เฟซที่ระบบคอมพิวเตอร์สองระบบใช้เพื่อแลกเปลี่ยนข้อมูลผ่านอินเทอร์เน็ตได้อย่างปลอดภัย) ใช้กุญแจเข้าถึง (access key) แบบ string เพื่อควบคุมการเข้าถึงข้อมูล

 บันทึกการเข้าถึงข้อมูล (Access logs): กิจกรรมทุกอย่างที่เกิดขึ้นใน Amazon S3 สามารถบันทึกไปยัง Bucket ที่แยกออกมาเพื่อการรวบรวมและวิเคราะห์ข้อมูลได้

2) RDS Access Controls

 DB Security Groups: เปรียบเหมือนกับ Security Groups ของ EC2/VPC บน AWS โดยเป็นการควบคุมการเข้าถึงทางเครือข่ายที่อนุญาตให้เข้าถึงเฉพาะพอร์ตของฐานข้อมูลที่ต้องการ

 IAM permissions: สามารถใช้เพื่อควบคุมการทำงานของ Amazon RDS แต่ละประเภทที่ผู้ใช้แต่ละคนสามารถเรียกใช้ได้ เช่น อนุญาตให้ผู้ใช้บางคนอ่านข้อมูลจากตารางได้อย่างเดียว