สรุปบทเรียนจากการพัฒนาความรู้

รอบการประเมินที่ 2
ปีงบประมาณ พ.ศ. 2568

หลักสูตร ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์

จัดทำโดย นายสันตชัย วรรณกูล
ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศมีบทบาทสำคัญต่อการดำเนินงานของหน่วยงานราชการ ความปลอดภัยทางไซเบอร์กลายเป็นปัจจัยสำคัญที่ไม่สามารถมองข้ามได้ การรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศไม่เพียงแต่เป็นการปกป้องทรัพย์สินทางดิจิทัลของหน่วยงาน แต่ยังเป็นการรักษาความน่าเชื่อถือในการให้บริการประชาชนและการดำเนินงานตามภารกิจของรัฐ

ความปลอดภัยของข้อมูล (Information Security) เป็นพื้นฐานสำคัญในการรักษาข้อจำกัดที่ได้รับอนุญาตในการเข้าถึงและเปิดเผยข้อมูล รวมถึงการปกป้องความเป็นส่วนตัวและข้อมูลที่เป็นกรรมสิทธิ์ของหน่วยงาน ขณะที่ไซเบอร์สเปซ (Cyberspace) หมายถึงพื้นที่เสมือนที่เกิดจากการเชื่อมต่อของคอมพิวเตอร์ ระบบเครือข่ายอินเทอร์เน็ต และอุปกรณ์ดิจิทัลต่างๆ เป็น "โลกดิจิทัล" ที่ผู้คน ข้อมูล และเทคโนโลยีโต้ตอบกันผ่านเครือข่าย

1. หลักการพื้นฐานด้านความปลอดภัยทางไซเบอร์ หลักการพื้นฐานด้านความปลอดภัยทางไซเบอร์ที่ใช้เป็นแนวทางในการรักษาความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย 3 องค์ประกอบหลัก

1.1 ความลับ (Confidentiality) การป้องกันไม่ให้ข้อมูลถูกเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต โดยวิธีการการเข้ารหัส (Encryption), การกำหนดสิทธิ์ (Access Control), การยืนยันตัวตนหลายปัจจัย (MFA) ตัวอย่าง เช่น ข้อมูลบัตรประจำตัวประชาชนถูกเข้ารหัส ไม่สามารถอ่านได้หากไม่มี key ที่ถูกต้อง

1.2 ความถูกต้องแม่นยำ (Integrity) การรับประกันว่าข้อมูลไม่ถูกแก้ไขหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาตโดยวิธีการ Hashing, Digital Signature, Version Control ตัวอย่าง เช่น ระบบฐานข้อมูลประชาชนต้องรับประกันว่าข้อมูลไม่ถูกแก้ไขโดยบุคคลที่ไม่มีสิทธิ์

1.3 ความพร้อมใช้งาน (Availability) ข้อมูลและระบบต้องพร้อมใช้งานเมื่อผู้มีสิทธิ์ต้องการ โดยวิธีการการสำรองข้อมูล (Backup), ความซ้ำซ้อน (Redundancy), การกระจายภาระงาน (Load Balancing), การป้องกัน DDoS ตัวอย่าง เช่น ระบบให้บริการออนไลน์ของหน่วยงานต้องเปิดให้บริการตลอด 24/7

2. ตัวอย่างการรักษาความปลอดภัยทางไซเบอร์

2.1 ความปลอดภัยเครือข่าย (Network Security) การปฏิบัติในการป้องกันเครือข่ายจากการเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานในทางที่ผิด การรบกวน หรือการหยุดชะงักของบริการ

2.2 ความปลอดภัยแอปพลิเคชัน (Application Security) กระบวนการที่เกี่ยวข้องกับการตรวจจับการซ่อมแซม และการเพิ่มความปลอดภัยของแอปพลิเคชันเพื่อป้องกันข้อมูลหรือโค้ดจากการถูกขโมยก่อนที่จะมีการเผยแพร่

2.3 ความปลอดภัยคลาวด์ (Cloud Security) การผสมผสานของนโยบาย การควบคุมขั้นตอน และเทคโนโลยีที่ทำงานร่วมกันเพื่อปกป้องโครงสร้างพื้นฐานและระบบบนคลาวด์

2.4 ความปลอดภัยโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Security) ชุดเครื่องมือพื้นฐานที่ให้บริการด้านความปลอดภัย เช่น เครื่องสแกนไวรัส ระบบป้องกันการบุกรุก ซอฟต์แวร์มัลแวร์

3. การจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์

3.1 ประเภทการควบคุมความปลอดภัยของข้อมูล

3.1.1 การควบคุมเชิงขั้นตอน (Procedural Controls) การควบคุมเหล่านี้ป้องกัน ตรวจจับหรือลดความเสี่ยงด้านความปลอดภัยต่อทรัพย์สินทางกายภาพ รวมถึงการศึกษาเพื่อตระหนักรู้เรื่องความปลอดภัย กรอบการทำงานด้านความปลอดภัย การฝึกอบรม การปฏิบัติตามกฎระเบียบ และแผนการตอบสนองต่อเหตุการณ์

3.1.2 การควบคุมการเข้าถึง (Access Controls) การควบคุมเหล่านี้กำหนดว่าใครมีสิทธิ์เข้าถึงและใช้ข้อมูลของหน่วยงานและเครือข่าย รวมถึงการกำหนดข้อจำกัดในการเข้าถึงทางกายภาพของอาคารและการเข้าถึงเสมือนเช่นการอนุญาตการเข้าถึงที่มีสิทธิพิเศษ

3.1.3 การควบคุมเชิงเทคนิค (Technical Controls) การควบคุมเหล่านี้เกี่ยวข้องกับการใช้การยืนยันตัวตนของผู้ใช้หลายปัจจัยเมื่อเข้าสู่ระบบ ไฟร์วอลล์ และซอฟต์แวร์ป้องกันไวรัส

3.1.4 การควบคุมตามกฎระเบียบ (Compliance Controls) การควบคุมเหล่านี้เกี่ยวข้องกับกฎหมายความเป็นส่วนตัวและมาตรฐานความปลอดภัยทางไซเบอร์ ต้องการการประเมินความเสี่ยงด้านความปลอดภัยของข้อมูลและบังคับใช้ข้อกำหนดด้านความปลอดภัยของข้อมูล

3.2 กระบวนการจัดการความเสี่ยง (Risk Management Process)

3.2.1 การระบุความเสี่ยง (Identifying Risk) การประเมินสภาพแวดล้อมขององค์กรเพื่อระบุความเสี่ยงในปัจจุบันหรือที่อาจเกิดขึ้นซึ่งอาจส่งผลกระทบต่อการดำเนินงาน

3.2.2 การประเมินความเสี่ยง (Assess Risk) การวิเคราะห์ความเสี่ยงที่ระบุได้เพื่อดูว่ามีแนวโน้มที่จะส่งผลกระทบต่อหน่วยงานมากแค่ไหนและผลกระทบอาจเป็นอย่างไร

3.2.3 การควบคุมความเสี่ยง (Control Risk) กำหนดวิธีการ ขั้นตอน เทคโนโลยี หรือมาตรการอื่น ๆ ที่สามารถช่วยให้หน่วยงานลดความเสี่ยงได้

3.2.4 การทบทวนการควบคุม (Review Controls) ประเมินอย่างต่อเนื่องว่าการควบคุมที่มีอยู่มีประสิทธิภาพสามารถลดความเสี่ยงได้มากแค่ไหน และเพิ่มหรือปรับการควบคุมตามความจำเป็น

4. แนวทางปฏิบัติที่ดีที่สุดเพื่อลดความเสี่ยง

4.1 โครงการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ การสร้างความตระหนักรู้และเสริมสร้างทักษะให้แก่บุคลากรในหน่วยงาน

4.2 การอัปเดตซอฟต์แวร์อย่างสม่ำเสมอ การรักษาซอฟต์แวร์และระบบปฏิบัติการให้อยู่ในเวอร์ชันล่าสุด

4.3 โซลูชันการจัดการการเข้าถึงแบบสิทธิพิเศษ (PAM) การควบคุมและจัดการบัญชีผู้ใช้ที่มีสิทธิพิเศษในระบบ

4.4 การตรวจสอบสิทธิ์การเข้าถึงแบบหลายปัจจัย (MFA) การเพิ่มชั้นความปลอดภัยในการเข้าถึงระบบ

4.5 การสำรองข้อมูลแบบไดนามิก การสำรองข้อมูลที่สำคัญอย่างสม่ำเสมอและทดสอบการกู้คืนข้อมูล

5. การจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management)

5.1 ความหมายและความสำคัญของ BCM การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management - BCM) เป็นกระบวนการเชิงรุกที่หน่วยงานใช้เพื่อเตรียมพร้อม วางแผน และตอบสนองต่อเหตุการณ์ที่อาจทำให้การดำเนินงานหยุดชะงัก เช่น ภัยธรรมชาติ ไฟไหม้ น้ำท่วม การโจมตีไซเบอร์ หรือการระบาดของโรค โดยองค์ประกอบหลักของ BCM ประกอบด้วย

5.1.1 Business Impact Analysis (BIA) การวิเคราะห์ผลกระทบทางธุรกิจเพื่อระบุกิจกรรมที่สำคัญและจำเป็นต่อการดำเนินงานของหน่วยงาน

5.1.2 Risk Assessment (RA) การประเมินความเสี่ยงที่อาจเกิดขึ้นและส่งผลกระทบต่อการดำเนินงาน

5.1.3 Business Continuity Plan (BCP) แผนรองรับความต่อเนื่อง เช่น การมีไซต์สำรองการทำงานจากสถานที่อื่น

5.1.4 Disaster Recovery Plan (DRP) แผนการกู้คืนระบบเทคโนโลยีสารสนเทศและข้อมูล

5.1.5 Training & Testing การฝึกซ้อมและทดสอบแผนเป็นประจำเพื่อให้มั่นใจว่าแผนสามารถใช้งานได้จริง

6. การจัดการเหตุการณ์ด้านความปลอดภัยและกรอบมาตรฐานสากล

6.1 การจัดการเหตุการณ์ด้านความปลอดภัยสามารถแบ่งออกเป็น 3 ระดับตามความรุนแรงและผลกระทบ

6.1.1 การจัดการเหตุการณ์ (Incident Management) เหตุการณ์เล็กๆ ที่สามารถควบคุมและแก้ไขได้ด้วยกระบวนการปกติ

6.1.2 การจัดการภาวะฉุกเฉิน (Emergency Management) เหตุการณ์ที่มีความรุนแรงมากขึ้น ต้องมีการระดมทรัพยากรเพิ่มเติม และอาจกระทบความปลอดภัยของบุคลากรหรือการดำเนินงาน

6.1.3 การจัดการภาวะวิกฤต (Crisis Management) เหตุการณ์รุนแรงขั้นสูงสุด มีผลกระทบต่อทั้งหน่วยงาน และอาจกระทบภาพลักษณ์ ความน่าเชื่อถือ กฎหมาย หรือการดำเนินงานของหน่วยงาน

7. มาตรฐานสากลที่เกี่ยวข้อง

7.1 มาตรฐาน ISO 22301: ระบบจัดการความต่อเนื่องทางธุรกิจ ISO 22301 เป็นมาตรฐานสากลสำหรับระบบจัดการความต่อเนื่องทางธุรกิจ ที่ให้กรอบการทำงานที่เป็นระบบและมีประสิทธิภาพ

7.2 มาตรฐาน ISO 27005: การจัดการความเสี่ยงด้านความปลอดภัยสารสนเทศ ISO 27005 เป็นมาตรฐานที่ให้แนวทางในการจัดการความเสี่ยงด้านความปลอดภัยสารสนเทศ โดยมุ่งเน้นการระบุ ประเมิน และจัดการความเสี่ยงผ่านกระบวนการที่เป็นระบบ

8. การบริหารความเสี่ยงด้านไซเบอร์

8.1 ผลกระทบ (Impact) ความเสียหายหรือผลกระทบที่อาจเกิดขึ้นต่อหน่วยงานหากเหตุการณ์เสี่ยงเกิดขึ้น

8.2 ความน่าจะเป็น (Likelihood) โอกาสหรือความถี่ที่เหตุการณ์เสี่ยงจะเกิดขึ้น

8.3 ภัยคุกคาม (Threat) อะไรก็ตามที่อาจก่อให้เกิดอันตรายหรือความเสียหายต่อทรัพย์สินหรือระบบ

8.4 ช่องโหว่ (Vulnerability) จุดอ่อนหรือข้อบกพร่องในระบบที่ภัยคุกคามสามารถใช้ประโยชน์ได้

ข้อสรุปและแนวคิดในการประยุกต์ใช้เพื่อพัฒนาองค์การ

ข้อสรุป

จากการศึกษาหลักการและแนวปฏิบัติด้านความปลอดภัยทางไซเบอร์ สามารถสรุปได้ว่า การรักษาความปลอดภัยข้อมูลในยุคดิจิทัลจำเป็นต้องมีการบูรณาการระหว่างเทคโนโลยี กระบวนการ และบุคลากรอย่างเป็นระบบ โดยหลัก CIA Triad ยังคงเป็นพื้นฐานสำคัญในการออกแบบระบบความปลอดภัย ขณะที่การจัดการความต่อเนื่องทางธุรกิจและการเตรียมพร้อมรับมือกับเหตุการณ์ไม่คาดคิดจะช่วยให้องค์กรสามารถดำเนินงานได้อย่างต่อเนื่องแม้ในสถานการณ์วิกฤต

แนวคิดในการประยุกต์ใช้เพื่อพัฒนาองค์กร

1. การพัฒนาแบบองค์รวม องค์กรควรนำหลักการความปลอดภัยทางไซเบอร์มาบูรณาการเข้ากับแผนยุทธศาสตร์องค์กร โดยไม่ถือเป็นเพียงเรื่องของหน่วยงาน IT เท่านั้น แต่เป็นความรับผิดชอบร่วมกันของทุกหน่วยงาน

2. การสร้างวัฒนธรรมความปลอดภัย การพัฒนาความตระหนักรู้และสร้างวัฒนธรรมความปลอดภัยให้กับบุคลากรทุกระดับ ผ่านการฝึกอบรมอย่างต่อเนื่องและการสร้างแรงจูงใจในการปฏิบัติตามมาตรการความปลอดภัย

3. การประยุกต์ใช้เทคโนโลยีที่เหมาะสม องค์กรควรเลือกใช้เทคโนโลยีและโซลูชันด้านความปลอดภัยที่เหมาะสมกับบริบทและความต้องการขององค์กร โดยคำนึงถึงความคุ้มค่าการลงทุนและความเสี่ยงที่ยอมรับได้

4. การพัฒนาขีดความสามารถในการตอบสนอง การจัดตั้งทีมตอบสนองต่อเหตุการณ์ด้านความปลอดภัย (Incident Response Team) และการฝึกซ้อมแผนรับมือกับสถานการณ์ต่างๆ อย่างสม่ำเสมอ เพื่อให้องค์กรสามารถรับมือกับภัยคุกคามได้อย่างรวดเร็วและมีประสิทธิภาพ

5. การปรับปรุงและพัฒนาอย่างต่อเนื่อง การนำหลักการ PDCA (Plan-Do-Check-Act) มาใช้ในการจัดการความปลอดภัยทางไซเบอร์ โดยมีการประเมินผล ปรับปรุง และพัฒนาระบบความปลอดภัยให้ทันต่อภัยคุกคามที่เปลี่ยนแปลงไปอย่างต่อเนื่อง

แหล่งที่มา

หลักสูตร : ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์ (Understanding Cybersecurity Risk Management)

ด้านการพัฒนา (ระบุ ✓) : ☑ ดิจิทัล
☐ ความรู้เฉพาะด้านเพื่อใช้ในการปฏิบัติงาน
☐ เพิ่มศักยภาพตนเอง/ประสิทธิภาพในการทำงาน

บรรยายโดย : ผศ.พิเศษ สันติพัฒน์ อรุณธารี

หน่วยงานผู้รับผิดชอบ : สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

วิธีการพัฒนาตนเอง : TDGA e-learning

วันที่ได้รับการฝึกอบรม : 25 ก.ค. 2568 **สถานที่ :** กรมพัฒนาที่ดิน