62010336 นายธนกร ชาญเชิงพานิช

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง พ.ศ. ๒๕๕๕

1. ในการสร้างความมั่นคงปลอดภัยด้านบริหารจัดการนั้น หน่วยงานต้องวางแผนการติดตามและประเมินผลการใช้งานความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ เพื่อปรับปรุงในกรณีมีการเปลี่ยนแปลงใด ๆ ภายในหน่วยงาน ทั้งนี้เพื่อให้เหมาะสมกับสถานการณ์การใช้งาน และคงความมีประสิทธิผลอยู่เสมอ

2. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศทั้งภายในและภายนอกหน่วยงานหรือองค์กรสามารถทำได้ดังนี้

2.1 มีการกำหนดเนื้องานหรือหน้าที่ความรับผิดชอบต่าง ๆ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศไว้อย่างชัดเจน

2.2 มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้าน หรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน

2.3 จัดให้มีการพิจารณาทบทวนแนวทางในการบริหารจัดการงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ในการดำเนินงาน ทั้งนี้การพิจารณาทบทวนดังกล่าว ควรดำเนินการโดยผู้ไม่มีส่วนได้เสียกับงานที่มีการพิจารณาทบทวน

3. การบริหารจัดการทรัพย์สินสารสนเทศ สามารถทำได้ดังนี้

3.1 มีการกำหนดบุคคลผู้มีหน้าที่ดูแลควบคุมการใช้งานและรับผิดชอบทรัพย์สินสารสนเทศไว้ชัดเจน

3.2 มีการกำหนดกฎระเบียบในการใช้งานทรัพย์สินสารสนเทศไว้อย่างชัดเจน โดยจัดทำเป็นเอกสารและมีการประกาศใช้ในหน่วยงาน เครื่องมือที่ใช้ในการจัดทำเอกสาร เช่น Microsoft Word

3.3 มีการจำแนกประเภทของข้อมูลสารสนเทศ โดยจำแนกตามมูลค่าของข้อมูล ข้อกำหนดทางกฎหมาย ระดับชั้นความลับและความสำคัญต่อหน่วยงาน เช่นการกำหนดสิทธิของผู้ใช้ในการเข้าถึงข้อมูลให้สามารถอ่านได้อย่างเดียว แต่ไม่สามารถแก้ไขข้อมูลได้ หรือกำหนดให้ผู้ใช้เข้าถึงข้อมูลในส่วนที่ถูกอนุญาติเท่านั้น

3.4 มีการกำหนดและประกาศใช้ขั้นตอนที่เหมาะสมในการจำแนกประเภทของข้อมูลสารสนเทศ และจัดการข้อมูลสารสนเทศโดยให้สอดคล้องกับแนวทางการจำแนกประเภทของข้อมูลสารสนเทศที่หน่วยงานประกาศใช้

4. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร พนักงาน หน่วยงานหรือ บุคคลภายนอกต้องได้รับการอบรมเพื่อสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตน และได้รับการสื่อสารให้ทราบถึงนโยบายหรือระเบียบปฏิบัติด้านความ มั่นคงปลอดภัยสารสนเทศที่หน่วยงานประกาศใช้อย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลง ในการอบรมนั้นนอกจากจะทำได้โดยการอบรมที่สถานที่จริง ปัจจุบันยังมีแอปพลิเคชันที่สามารถจัดการอบรมแบบออนไลน์ได้ เช่น Zoom, Microsoft Team, Google Meet

5. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อมสามารถทำได้ดังนี้

5.1 มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันพื้นที่หรือสถานที่ ปฏิบัติงาน หรืออุปกรณ์สารสนเทศต่าง ๆ เช่นการติดตั้งถังดับเพลิงไว้เผื่อกรณีที่เกิดไฟไหม้ขึ้น, การติดอุปกรณ์ทำความเย็นไว้ในห้อง Server, การติดตั้งเครื่องสำรองไฟในกรณีที่ไฟฟ้าดับ

5.2 ไม่ควรนำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของหน่วยงานหากมิได้รับอนุญาต วิธีการป้องกันคือกำหนด Policy ของ Firewall ไม่ให้มีการส่งข้อมูลสำคัญออกสู่ภายนอก

6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์และระบบสารสนเทศ สามารถทำได้ดังนี้

6.1 มีการจัดการควบคุมการเปลี่ยนแปลงของระบบสารสนเทศ

6.2 มีการติดตามผลการใช้งานทรัพยากรสารสนเทศ และวางแผนด้านทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม สามารถทำได้โดยการใช้ Network Monitoring Tools ได้แก่ SolarWinds, Atera, LogicMonitor เป็นต้น

6.3 มีขั้นตอนการปฏิบัติงานในการจัดการและจัดเก็บข้อมูลสารสนเทศเพื่อมิให้ข้อมูลรั่วไหลหรือถูกนำไปใช้ผิดประเภท

6.4 มีการจัดเก็บ Log ที่เกี่ยวข้องกับข้อผิดพลาดใด ๆ ของระบบสารสนเทศ มีการวิเคราะห์ Log ดังกล่าว อย่างสม่ำเสมอ และมีการจัดการแก้ไขข้อผิดพลาดที่ตรวจพบอย่างเหมาะสม สามารถใช้เครื่องมือจัดการ Log ได้ เช่น Sematext Logs, SolarWinds Loggly, Splunk เป็นต้น

6.5 ระบบเวลาของระบบสารสนเทศต่าง ๆ ที่ใช้ในหน่วยงานหรือในขอบเขตงานด้านความมั่นคงปลอดภัย (Security domain) ต้องมีความสอดคล้องกัน (Synchronization) โดยให้มีการตั้งค่าพร้อมกับเวลาจากแหล่งเวลาที่เชื่อถือได้ แหล่งเวลาที่น่าเชื่อถือได้ของประเทศไทยนั้น ได้แก่ เวลามาตรฐานประเทศไทย โดยกรมอุทกศาสตร์ กองทัพเรือ http://www.time2.navy.mi.th/

7. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ระบบคอมพิวเตอร์ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์และข้อมูลคอมพิวเตอร์ สามารถทำได้ดังนี้

7.1 มีข้อบังคับให้ผู้ใช้งานปฏิบัติตามขั้นตอนเพื่อการเลือกใช้รหัสผ่านอย่างมั่นคงปลอดภัยตามที่หน่วยงานกำหนด

7.2 ผู้ใช้งานสามารถเข้าถึงเฉพาะบริการทางเครือข่ายคอมพิวเตอร์ที่ตนเองได้รับอนุญาตให้ใช้ได้เท่านั้น เครื่องมือที่ใช้ได้แก่ Firewall โดยการกำหนด Policy เพื่อให้สิทธิแก่ผู้ใช้งาน

7.3 ให้มีการกำหนดวิธีการตรวจสอบตัวตนที่เหมาะสมเพื่อควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกล ได้แก่การใช้งาน Two-factor authentication เช่น Google Authenticator, YubiKey เป็นต้น

7.4 มีการควบคุมการเข้าถึงช่องทางการดูแลระบบสารสนเทศทั้งทางกายภาพและการเชื่อมต่อผ่านคอมพิวเตอร์สำหรับระบบสารสนเทศที่สามารถเข้าถึงจากระยะไกลได้เช่น Remote diagnostic หรือ Configuration facility ของอุปกรณ์เครือข่ายคอมพิวเตอร์ ตัวอย่างการป้องกัน ได้แก่ การกำหนด Policy Firewall ให้มีการเชื่อมต่อจากอุปกรณ์ที่ได้รับการอนุญาติสามารถเชื่อมต่อได้เท่านั้น

7.5 มีการจัดกลุ่มตามประเภทของข้อมูลสารสนเทศที่ให้บริการ ระบบสารสนเทศ กลุ่มผู้ใช้งานโดยมีการ แบ่งแยกบนเครือข่ายคอมพิวเตอร์อย่างเป็นสดส่วน เช่น การกำหนด VLAN ให้แต่แผนกบนเครือข่าย

7.6 กำหนดให้มีการควบคุมเส้นทางการไหลของข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์เพื่อไม่ให้ขัดแย้งกับนโยบายควบคุมการเข้าถึงของแอพพลิเคชั่น เช่นการ config เครือข่ายบน Router และ Switch

7.7 กำหนดขั้นตอนการ Log-on เพื่อควบคุมการเข้าถึงระบบปฏิบัติการคอมพิวเตอร์

7.8 ให้จัดทำหรือจัดให้มีระบบการบริหารจัดการรหัสผ่านที่สามารถทำงานแบบเชิงโต้ตอบกับผู้ใช้งาน (Interactive) และสามารถรองรับการใช้งานรหัสผ่านที่มีความมั่นคงปลอดภัย ตัวอย่างโปรแกรมที่ใช้จัดการรหัสผ่านในปัจจุบัน ได้แก่ Bitwarden, Keeper, LastPass เป็นต้น

8. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ระบบ คอมพิวเตอร์ระบบงานคอมพิวเตอร์และระบบสารสนเทศ สามารถทำได้ดังนี้

8.1 ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ ที่จะรับเข้าสู่แอพพลิเคชั่นก่อนเสมอ เพื่อให้มั่นใจได้ว่าข้อมูลมีความถูกต้องและมีรูปแบบเหมาะสม

8.2 ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ อันเป็นผลจากการประมวลผลของแอพพลิเคชั่นเพื่อให้มั่นใจได้ว่าข้อมูลที่ได้จากการประมวลผลถูกต้องและเหมาะสม

8.3 จัดให้มีแนวทางการบริหารจัดการกุญแจ (Key) เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับของหน่วยงาน เช่นการใช้บริการ Amazon Key Management Service (KMS) เพื่อบริหารและจัดเก็บ Key ผ่านระบบ Cloud

8.4 ให้เลือกชุดข้อมูลสารสนเทศที่จะนำไปใช้เพื่อการทดสอบในระบบสารสนเทศอย่างระมัดระวัง รวมทั้งมีแนวทางควบคุมและป้องกันข้อมูลรั่วไหล

8.5 ให้มีการจำกัดการเข้าถึงซอร์สโค้ด (Source code) ของโปรแกรม เช่นการใช้ GitHub, Amazon Code Commit เพื่อจัดเก็บซอร์สโค้ด

8.6 หากมีการเปลี่ยนแปลงใด ๆ ในระบบปฏิบัติการคอมพิวเตอร์ให้มีการตรวจสอบทบทวนการทำงาน ของโปรแกรมที่มีความสำคัญ และทดสอบการใช้งานเพื่อให้มั่นใจว่าผลของการเปลี่ยนแปลงดังกล่าวจะไม่ส่งผล กระทบใด ๆ ต่อความมั่นคงปลอดภัยของระบบสารสนเทศและการให้บริการของหน่วยงาน สามารถทำได้โดยการเขียน Unit Test, Integration Test และ End-2-End Test เช่นการใช้ Library Testify ของ Golang ในการทำ Unit Test, การทดสอบโดยการยิง API ผ่าน Postman เพื่อตรวจสอบว่า API มีการทำงานที่ถูกต้องหรือไม่

9. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง สามารถทำได้ดังนี้

9.1 จัดให้มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่จำเป็น โดยกำหนดให้เป็นส่วนหนึ่งของขั้นตอนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน

9.2 กำหนดให้มีกรอบงานหลักสำหรับการพัฒนาแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน เพื่อให้การพัฒนาแผนต่าง ๆ เป็นไปในทิศทางเดียวกัน รวมทั้งสอดคล้องกับข้อกำหนดด้านความ มั่นคงปลอดภัย ตลอดจนมีการจัดลำดับความสำคัญก่อนหลังในการทดสอบและการดูแล

9.3 ให้มีการทดสอบและปรับปรุงแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน อย่างสม่ำเสมอ เพื่อให้มั่นใจว่าแผนดังกล่าวเป็นปัจจุบันและมีประสิทธิผลอยู่เสมอ ตัวอย่างเครื่องมือที่ใช้ในการจัดการ ได้แก่ IBM Security QRadar SIEM, Blumira Automated Detection & Response เป็นต้น

10. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์หรือกระบวนการ ใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ สามารถทำได้ดังนี้

10.1 จัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน

10.2 ใช้เทคนิคการเข้ารหัสลับ ที่สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน ตัวอย่างอัลกอริทึมที่ใช้ในการเข้ารหัสลับ ได้แก่ Advanced Encryption Standard (AES), RSA เป็นต้น

10.3 ให้มีการทบทวนตรวจสอบระบบสารสนเทศในด้านเทคนิคอย่างสม่ำเสมอเพื่อให้สอดคล้องกับมาตรฐานการพัฒนางานด้านความมั่นคงปลอดภัยด้านสารสนเทศ เครื่องมือที่ใช้ในการดูประสิทธิภาพของเครื่องคอมพิวเตอร์ ได้แก่ NZXT CAM, HWiNFO, HWMonitor เป็นต้น

10.4 วางแผนและจัดให้มีข้อกำหนดการตรวจสอบและกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ เพื่อลดความเสี่ยงในการเกิดการหยุดชะงักของการให้บริการ

10.5 ป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise) เช่นการตั้งรหัสผ่านเครื่องมือที่ใช้ในการตรวจสอบให้มีความแข็งแรง