Digital Government Development Agency (DGA)

วิธีปฏิบัติงาน
ด้านความมั่นคงปลอดภัยไซเบอร์ภาครัฐ
Practices for Government Cybersecurity

2567

สารบัญ

สารบัญตารางแบบประเมิน

บทนำ

เอกสารวิธีปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ภาครัฐ (Practices for Government Cybersecurity) ฉบับนี้มีวัตถุประสงค์เพื่อใช้เป็นแนวทางเบื้องต้นแก่หน่วยงานภาครัฐให้เกิดการพัฒนาบริการภาครัฐที่มีความมั่นคงปลอดภัย และน่าเชื่อถือ ซึ่งหน่วยงานภาครัฐสามารถเรียนรู้เอกสารฉบับนี้ และนำไปพัฒนากระบวนการทางดิจิทัลที่มีประสิทธิภาพ มีหลักอ้างอิงในการปฏิบัติงานอย่างมีมาตรฐาน ก่อให้เกิดความมั่นคงปลอดภัย และน่าเชื่อถือแก่หน่วยงานภาครัฐ นอกจากนี้ ยังมีวัตถุประสงค์เพื่อให้หน่วยงานภาครัฐมีการจัดทำกระบวนการ หรือการดำเนินงานทางดิจิทัล มีการให้บริหารราชการแผ่นดิน และการให้บริการประชาชนให้เป็นไปตามกฎหมายที่เกี่ยวข้องเช่น พระราชบัญญัติการบริหารงาน และการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นต้น ซึ่งกฎหมายเหล่านี้ได้มีการกำหนดขึ้นเพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพ และเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐ และประชาชนที่ใช้บริการ

เอกสารฉบับนี้จะอธิบายแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ โดยแยกเป็นหัวข้อต่าง ๆ เช่น การประเมินความเสี่ยง การรับมือภัยคุกคามทางไซเบอร์ กรอบมาตรฐานที่ประกอบไปด้วยการระบุความเสี่ยง (Identify) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) มาตรการตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) และมาตรการรักษา และฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover) รวมไปถึง ข้อแนะนำเพิ่มเติมทางเทคนิคสำหรับผู้ดูแลระบบ และนักพัฒนาระบบ และข้อแนะนำสำหรับบุคลากรที่เป็นผู้ใช้งานทั่วไปอีกด้วย ในบางหัวข้อจะมีแนวทางในการประเมินตนเองเพื่อวัดระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ในหัวข้อนั้น ๆ

จากหัวข้อเนื้อหาข้างต้น จะเห็นได้ว่าผู้อ่านจะต้องให้ความสำคัญกับทุกหัวข้อตั้งแต่การระบุความเสี่ยง (เช่นการทำทะเบียนทรัพย์สิน หรือระบบสารสนเทศที่มีอยู่ การประเมินความเสี่ยง และกลยุทธ์ เป็นต้น) การป้องกัน ไปจนถึงการเผชิญเหตุ และการฟื้นฟู ซึ่งจะเปลี่ยนไปจากแนวคิดดั้งเดิมที่ผู้ปฏิบัติอาจจะให้ความสำคัญแต่การป้องกันเพียงอย่างเดียว เพราะจากกรณีศึกษาภัยคุกคามไซเบอร์ในช่วงหลายปีที่ผ่านมานี้ แม้ว่าหน่วยงานจะมีมาตรการที่ป้องกันเป็นอย่างดีตามมาตรฐานสากล แต่หน่วยงานเหล่านั้นก็ยังจะต้องเผชิญต่อภัยคุกคามอยู่ดี ซึ่งสามารถเกิดได้จากเหตุสุดวิสัย หรือภัยธรรมชาติที่ไม่สามารถป้องกันได้ ดังนั้น มาตรการอื่น ๆ อย่างการเผชิญเหตุเพื่อตอบสนอง และการฟื้นฟูก็มีความสำคัญไม่ยิ่งหย่อนกัน

เนื้อหาในเอกสารฉบับนี้ จะอ้างอิงตามเอกสาร หรือมาตรฐานที่ได้รับการยอมรับในระดับประเทศและนานาชาติ โดยจะอ้างอิงเป็นหลักจากประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 ซึ่งพัฒนาโดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) (***ในเอกสารฉบับนี้ เนื้อหาที่ยกมาจากประมวลแนวทางปฏิบัติ และกรอบมาตรฐานดังกล่าว จะเขียนเป็นตัวเอน***)

นอกจากนี้ เอกสารฉบับนี้ยังอ้างอิงจากเอกสารอื่น ๆ เพิ่มเติม โดยเฉพาะในบางหัวข้อที่มีเนื้อหาเฉพาะทางเทคนิค หรือเฉพาะกลุ่ม ซึ่งเอกสารอ้างอิงดังกล่าวประกอบไปด้วย

- NIST Cybersecurity Framework
- มาตรฐาน ISO/IEC 27001:2022
- มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล และมาตรฐานรัฐบาลดิจิทัลในส่วนที่เกี่ยวข้อง
- ISC2 Center for Cyber Safety and Education
- Cloud Security Alliance (CCSK Guide)
- Open Web Application Security Project (OWASP)
- Cybersecurity and Infrastructure Security Agency (CISA)

ในส่วนท้ายของบางหัวข้อ จะมีแนวทางการประเมินตนเองที่สรุปจากเนื้อหาในแต่ละหัวข้อเพื่อให้หน่วยงานได้ประเมินตนเอง ซึ่งการประเมินตนเองในแต่ละข้อจะเป็นคำถามที่ต้องการคำตอบเพียงใช่หรือไม่ใช่เท่านั้น และเป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้น ซึ่งหน่วยงานที่มีความพร้อมควรจะมีการประเมินเป็น “ใช่” ครบทุกข้อ และหากข้อใดมีคำตอบเป็น “ไม่ใช่” หน่วยงานควรจะมีการดำเนินในข้อนั้นอย่างเหมาะสม ไม่ว่าจะดำเนินการเอง หรือโดยผู้เชี่ยวชาญภายนอก หรืออย่างน้อยควรที่จะมีการวางแผนการดำเนินดังกล่าวในอนาคตโดยเร็ว สำหรับหน่วยงานขนาดเล็กที่อาจมีข้อจำกัดในเรื่องของความพร้อมและมีการประเมินเป็น “ไม่ใช่” ในหลายข้อ สามารถศึกษาเพิ่มเติมแนวทางเฉพาะสำหรับหน่วยงานขนาดเล็กได้จาก NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide

เนื้อหาดังกล่าวโดยส่วนใหญ่ในเอกสารฉบับนี้ เหมาะสำหรับผู้อ่านทุกระดับในหน่วยงานของรัฐ ตั้งแต่ผู้ที่มีความรู้ด้านเทคโนโลยีสารสนเทศในระดับที่สูงจนถึงระดับพื้นฐาน และตั้งแต่ระดับผู้บริหารจนถึงระดับปฏิบัติการ หรือผู้ใช้ทั่วไป แต่จะมีเนื้อหาทางเทคนิคบางส่วนที่ออกแบบไว้สำหรับผู้พัฒนาระบบ และผู้ดูแลระบบโดยเฉพาะซึ่งจะระบุไว้ที่หน้าแรกของหัวข้อนั้น

เอกสารฉบับนี้เหมาะที่จะใช้เป็นแนวทางเบื้องต้นในการกำหนดความต้องการพื้นฐานขั้นต่ำในการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานภาครัฐขนาดเล็ก หรือกลางขึ้นไป หากหน่วยงานใดมีมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ในระดับที่สูงกว่าเอกสารฉบับนี้อยู่แล้ว ก็ควรที่จะยึดตามมาตรการที่มีระดับความมั่นคงปลอดภัยไซเบอร์สูงกว่าเสมอตามความต้องการของหน่วยงานนั้น การกำหนดระดับความเข้มข้นของความมั่นคงปลอดภัยไซเบอร์นั้น ขึ้นอยู่กับบริบทของหน่วยงาน ซึ่งหน่วยงานนั้นจะต้องมีการวิเคราะห์ความต้องการพื้นฐาน และความเสี่ยงของหน่วยงานนั้นก่อนเสมอซึ่งการวิเคราะห์ความเสี่ยงจะมีการกล่าวถึงในเอกสารฉบับนี้

1. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment)

ในแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์นั้น ผู้ปฏิบัติไม่ใช่เพียงแต่มีมาตรการป้องกันภัยคุกคาม แต่ยังต้องมีมุมมองให้เห็นภาพรวมในด้านอื่น ๆ ด้วย โดยเฉพาะเรื่องความเสี่ยงด้านไซเบอร์และความเสี่ยงของหน่วยงาน หากหน่วยงานไม่มีการประเมินความเสี่ยง นั่นหมายถึงหน่วยงานจะไม่สามารถประเมินปัญหา หรือผลกระทบที่เกิดจากภัยคุกคามได้เลย ไม่ว่าจะเป็นผลจากความเสี่ยงด้านไซเบอร์ เช่นระบบโดนโจมตี ข้อมูลรั่วไหล บริการล่ม และผลจากความเสี่ยงของหน่วยงาน รวมถึงปัจจัยภายนอกอย่างกฎระเบียบ และปัจจัยด้านเศรษฐกิจ ซึ่งส่งผลกระทบทั้งด้านชื่อเสียง และเงินทอง การประเมินความเสี่ยงจึงเสมือนเป็นการทำให้หน่วยงานรู้จักจุดอ่อน จัดลำดับความสำคัญ ลดผลกระทบ เปลี่ยนจากมุมมองในการป้องกันภัยเพียงอย่างเดียวเป็นการประเมินเชิงรุก เพื่อสร้างความมั่นใจแก่หน่วยงาน และผู้มีส่วนได้เสีย

ขั้นตอนปฏิบัติ

เพื่อให้หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ และต่อเนื่อง หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ครอบคลุมเรื่องโครงสร้างองค์กร และบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติ และกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้ (อ้างอิงจาก ข้อที่ 18 ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564)

1.1. การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงประกอบไปด้วย 3 ขั้นตอน ดังนี้

1.1.1. การระบุความเสี่ยง (Risk Identification)

ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก การระบุความเสี่ยงประกอบไปด้วย

- การกำหนดขอบเขตที่ชัดเจนของการประเมินความเสี่ยง เช่น กำหนดขอบเขตของระบบสารสนเทศ ฮาร์ดแวร์ ข้อมูล และขั้นตอนปฏิบัติ เป็นต้น

- การรวบรวมข้อมูลจากผู้มีส่วนได้เสีย รวมถึงการระบุผู้มีส่วนได้เสียหลักให้ครบถ้วน เนื่องจากกลุ่มบุคคลดังกล่าวจะเป็นผู้ได้รับผลกระทบหลักจากความเสี่ยง จึงสามารถให้ข้อมูลความเสี่ยงได้ตรงกับความเป็นจริงมากที่สุด
- การวิเคราะห์ภัยคุกคาม หรือเหตุการณ์ที่เกือบเกิดภัยคุกคาม (Near Miss) ในอดีต เพื่อศึกษารูปแบบ (Pattern) ของภัยคุกคามที่อาจจะเกิดในอนาคต
- การเลือกใช้เครื่องมือสำหรับการประเมินความเสี่ยงที่เหมาะสม โดยพิจารณาจากวิธีดังต่อไปนี้
  - **ข้อมูลสถิติ** เป็นการนำข้อมูลสถิติย้อนหลังของการเกิดความเสี่ยงทั้งที่เกิดขึ้นกับหน่วยงาน และที่มีการเปิดเผยข้อมูลจากหน่วยงานที่เชื่อถือได้ นำมาใช้ในการระบุความเสี่ยงที่อาจจะเกิดขึ้นได้
  - **ทะเบียนความเสี่ยง (Risk Register)** เป็นการนำความเสี่ยงที่หน่วยงานได้มีการจัดทำทะเบียนความเสี่ยงไว้นำมาพิจารณาความเสี่ยงที่อาจจะเกิดขึ้นได้
  - **การวิเคราะห์สวอต (SWOT Analysis)** เป็นการประยุกต์ใช้จากการวิเคราะห์สวอตโดยนำผลของการวิเคราะห์ในส่วนของ ภัยคุกคาม (Threat) และ จุดอ่อน (Weakness) มาพิจารณาระบุความเสี่ยงที่อาจจะเกิดขึ้นได้
  - **ระบบติดตาม และป้องกันภัย** เป็นการนำข้อมูลที่ได้จากเครื่องมือที่ติดตั้งในระบบเทคโนโลยีสารสนเทศมาระบุความเสี่ยง เช่น Network Monitor, IPS/IDS, Firewall, Security Event and Incident Management (SEIM) และ Log Analysis เป็นต้น
  - **ปรึกษาผู้เชี่ยวชาญ** เป็นการขอรับการปรึกษาจากผู้เชี่ยวชาญในการเอามาวิเคราะห์และระบุความเสี่ยงของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่อาจจะเกิดขึ้นได้
- การวิเคราะห์ปัจจัยภายนอก เช่น กฎหมาย หรือระเบียบที่เกี่ยวข้อง แนวโน้มการตลาด หรือเหตุการณ์ทางการเมือง ที่อาจส่งผลกระทบต่อการดำเนินงานของหน่วยงาน

1.1.2. การวิเคราะห์ความเสี่ยง (Risk Analysis)

ต้องเข้าใจ และวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม ซึ่งประกอบไปด้วย

- การประเมินโอกาสที่จะเกิด และผลกระทบของความเสี่ยง
- การวัดระดับความเสี่ยง ทั้งการวัดในเชิงปริมาณ และเชิงคุณภาพ เช่น ความสูญเสียทางด้านการเงิน การเสื่อมเสียทางชื่อเสียงของหน่วยงาน หรือการดำเนินงานของหน่วยงานที่สะดุด หรือไม่ราบรื่น
- การเลือกผู้เชี่ยวชาญมาให้คำปรึกษา และร่วมวิเคราะห์ความเสี่ยงเฉพาะด้าน โดยพิจารณาจากประสบการณ์ ความน่าเชื่อถือ ผลงานอ้างอิง รวมถึงประกาศนียบัตร (Certificate) ที่เกี่ยวข้องที่เป็นที่ยอมรับในระดับชาติหรือระดับสากล เช่น Certified Information Systems Security

Professional (CISSP), Certified Information Systems Auditor (CISA), ISO/IEC 27001 Lead Auditor, เป็นต้น

1.1.3. การประเมินค่าความเสี่ยง (Risk Evaluation)

ต้องประเมินถึงผลของการวิเคราะห์ความเสี่ยงว่าความเสี่ยงที่ระบุไว้นั้น อยู่ในระดับที่ยอมรับได้ หรือไม่ หรือมีผลกระทบต่อหน่วยงานมากน้อยเพียงใด โอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้น และผลกระทบต่อการปฏิบัติงาน และการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

- การจัดลำดับความสำคัญของความเสี่ยง โดยคำนึงถึงผลกระทบที่สำคัญ และโอกาสที่จะเกิด
- การกำหนดระดับความเสี่ยงที่เหลืออยู่ที่ยอมรับได้ โดยคำนึงถึงผลกระทบของหน่วยงานเป็นหลัก
- การทบทวนวิธีลดความเสี่ยงในปัจจุบันว่ามีประสิทธิภาพ หรือให้ผลลัพธ์ที่อยู่ในระดับที่รับได้ หรือไม่
- การจัดทำบันทึกเอกสาร และแผนการปฏิบัติการในการจัดการความเสี่ยง

1.2. การจัดการความเสี่ยง (Risk Treatment)

ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยง และผลประโยชน์ที่คาดว่าจะได้รับ นอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตาม และทบทวนความเสี่ยง

- การตัดสินใจในการจัดการความเสี่ยง โดยนำผลการประเมินความเสี่ยงมาพิจารณาว่าจะตัดสินใจอย่างไรกับความเสี่ยงนี้ ได้แก่ การยอมรับความเสี่ยง (Risk Acceptance) การลดความเสี่ยง (Risk Reduction) การถ่ายโอนความเสี่ยง (Risk Transfer) และการหลีกเลี่ยงความเสี่ยง (Risk Avoidance)
- การวัดระดับความเสี่ยงที่เหลืออยู่ เพื่อวิเคราะห์ว่าอยู่ในระดับที่ยอมรับได้ หรือไม่
- การประเมินระดับความเสี่ยงที่เหลืออยู่ และเปรียบเทียบกับความเสี่ยงที่เคยคาดการณ์ไว้
- การสื่อสารผลของการประเมินความเสี่ยงกับผู้มีส่วนได้เสีย เพื่อให้ผู้มีส่วนได้เสียเข้าใจถึงภาพรวมความเสี่ยงของหน่วยงาน และเพื่อความโปร่งใสของหน่วยงาน
- การกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ รวมถึงการกำหนดดัชนีชี้วัดที่ยอมรับได้ และสามารถอธิบายถึงการกำหนดช่วงดังกล่าวได้ โดยให้พิจารณาที่เป้าหมายของการจัดการกับความเสี่ยงที่กำลังถูกนำมา

พิจารณา โดย KRI ที่กำหนดควรสอดคล้องกับความต้องการของผู้บริหารของหน่วยงาน และทรัพยากรที่ถูกจัดสรรในการดำเนินงานในการที่นำมาใช้จัดการกับความเสี่ยง ตัวอย่างการกำหนด KRI เช่น

- จำนวนความพยายามที่สำเร็จของการบุกรุกระบบเทคโนโลยีสารสนเทศของหน่วยงานต้องไม่เกิน 2 ครั้งต่อปี
- ระยะเวลาในการตอบสนองต่อเหตุการณ์ละเมิดความมั่นคงปลอดภัยที่ไม่สอดคล้องตาม (Service Level Agreement: SLA) ที่กำหนด ต้องไม่เกิน 10% ในรอบ 3 เดือน
- ระยะเวลาในการแก้ไขปัญหาของเหตุการณ์ละเมิดความมั่นคงปลอดภัยที่ไม่สอดคล้องตาม SLA ที่กำหนด ต้องไม่เกิน 10% ในรอบ 3 เดือน
- ความล้มเหลวในการอัพเดตระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่ายที่ดูแลรับผิดชอบ ต้องไม่เกิน 10% ต่อการอัพเดตในแต่ละครั้ง
- ความล้มเหลวในการอัพเดตโปรแกรม Antivirus ของเครื่องคอมพิวเตอร์แม่ข่ายที่ดูแลรับผิดชอบ ต้องไม่เกิน 10% ต่อการอัพเดตในแต่ละครั้ง

1.3. การติดตาม และทบทวนความเสี่ยง (Risk Monitoring and Review)

ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

- การกำหนดช่วงเวลาการติดตาม และทบทวนความเสี่ยงที่ชัดเจน โดยให้สอดคล้องกับภารกิจและวัตถุประสงค์ของหน่วยงาน
- การกำหนดตัวชี้วัดผลงาน (Key Performance Indicator : KRI) เพื่อชี้วัดผลสำเร็จของการจัดการความเสี่ยง
- การเลือกใช้เทคโนโลยี หรือเครื่องมือที่เหมาะสมในการติดตามความเสี่ยง
- การประเมินความเสี่ยงเป็นระยะเพื่อประเมินหาความเสี่ยงใหม่ ๆ และการประเมินความเสี่ยงเดิมซ้ำ
- การทบทวนประสิทธิภาพของการจัดการความเสี่ยงที่ผ่านมา
- การให้ผู้มีส่วนได้เสียมาร่วมทบทวนการจัดการความเสี่ยงของหน่วยงาน
- การบันทึกเอกสารเกี่ยวกับการเปลี่ยนแปลงใด ๆ ในการจัดการความเสี่ยง

1.4. การรายงานความเสี่ยง (Risk Reporting)

ต้องรายงานระดับความเสี่ยง และผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการของหน่วยงาน หรือผู้บริหารที่ได้รับมอบหมาย ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติ และกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง

และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

โดยหน่วยงานต้องดำเนินการกรณีมีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ดังนี้

- การจัดทำรายงาน และวิธีสื่อสารที่แตกต่างกันไปยังผู้มีส่วนได้เสียเฉพาะกลุ่มที่แตกต่างกัน
- การจัดทำรายงานความเสี่ยงเพื่อสื่อสารไปยังคณะกรรมการของหน่วยงาน
- การจัดทำบทสรุปสำหรับผู้บริหารเพื่อสื่อสารไปยังผู้บริหารของหน่วยงาน
- การจัดทำสื่อที่สามารถเข้าใจได้ง่าย เช่น กราฟ หรือแผนภูมิ
- การกำหนดช่วงเวลาในการรายงาน และสื่อสารไปยังผู้มีส่วนได้เสีย เพื่อให้ผู้มีส่วนได้เสียได้รับทราบเป็นระยะ และเพื่อให้เกิดความโปร่งใสของหน่วยงาน
- การประชาสัมพันธ์ถึงผลลัพธ์ของการลดความเสี่ยงที่ประสบความสำเร็จตามแผน เพื่อยืนยันว่าการจัดการความเสี่ยงเป็นไปในแนวทางที่ถูกต้อง
- การถอดบทเรียนจากการจัดการความเสี่ยง และภัยคุกคามที่เกิดขึ้นในอดีต

ตารางที่ 1 แบบประเมินตนเองด้านการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้น ซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. หน่วยงานได้มีการระบุความเสี่ยงที่สำคัญทั้งหมด และบันทึกความเสี่ยงดังกล่าวลงในเอกสาร หรือไม่		
2. หน่วยงานมีขั้นตอน หรือกระบวนการในการวิเคราะห์โอกาสที่จะเกิด และผลกระทบความเสี่ยง หรือไม่		
3. หน่วยงานมีแผนปฏิบัติการในการจัดการความเสี่ยง หรือไม่		
4. หน่วยงานมีขั้นตอน หรือกระบวนการในการระบุ หรือจัดการความเสี่ยงที่เหลืออยู่ หรือไม่		
5. หน่วยงานมีการกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) หรือไม่		
6. หน่วยงานมีการกำหนดช่วงเวลาในการติดตาม และทบทวนความเสี่ยง หรือไม่		
7. หน่วยงานมีการจัดทำรายงานความเสี่ยงที่แตกต่างกันสำหรับผู้มีส่วนได้เสียที่แตกต่างกัน หรือไม่		
8. หน่วยงานได้ผนวกเรื่องการจัดการความเสี่ยงเข้ากับเรื่องกระบวนการตัดสินใจของผู้บริหาร หรือไม่		
9. หน่วยงานได้ช่องทางการสื่อสารเรื่องความเสี่ยงแก่ผู้มีส่วนได้เสีย หรือไม่		
10. หน่วยงานมีขั้นตอน หรือกระบวนการในการปรับปรุงการจัดการความเสี่ยง โดยคำนึงจากการถอดบทเรียนที่ได้ และผลตอบรับจากผู้มีส่วนได้เสีย หรือไม่		

2. ความสามารถในการเตรียมตัว และตอบสนองต่อภัยคุกคามทางไซเบอร์ (Cyber Resilience)

ในโลกดิจิทัลที่ภัยไซเบอร์ได้สร้างผลกระทบทั้งทางเศรษฐกิจ และสังคมมากขึ้นในช่วงหลายปีที่ผ่านมานี้ หน่วยงานต่าง ๆ จำเป็นจะต้องมีแผนการรับมือเหตุการณ์ด้านความปลอดภัยไซเบอร์ แผนการรับมือนี้ไม่ได้เป็นเพียงแค่เครื่องมือที่ใช้ป้องกันภัยไซเบอร์ แต่ยังเป็นกระบวนการลดความเสี่ยง และความเสียหายอย่างเป็นระบบ ตั้งแต่การเตรียมความพร้อม การซักซ้อมแผน การป้องกัน การตรวจจับ การวิเคราะห์ การตอบสนอง และการฟื้นฟูจากเหตุภัยคุกคามอย่างรวดเร็ว นอกจากนี้แผนดังกล่าว ยังช่วยให้หน่วยงานปฏิบัติตามนโยบาย กฎระเบียบ ช่วยในกระบวนการการตัดสินใจ และสร้างความเชื่อมั่นต่อผู้มีส่วนได้เสีย ดังนั้น หน่วยงานที่ไม่มีแผนการรับมือ อาจต้องเผชิญต่อความเสี่ยงต่อการที่ข้อมูลถูกละเมิด รวมถึงผลกระทบต่อชื่อเสียง เศรษฐกิจ และอาจส่งผลทางกฎหมายได้ การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ จึงเป็นสิ่งจำเป็นสำหรับหน่วยงานทุกประเภทในการปกป้องตนเองในโลกดิจิทัลจากภัยคุกคามทางไซเบอร์

การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์นั้น สอดคล้องกับแนวคิดใหม่ที่ว่าแม้ว่าหน่วยงานจะมีวิธีปฏิบัติในการป้องกันภัยทางไซเบอร์ที่ดีเพียงใด ก็ยังเกิดโอกาสถูกโจมตีได้เสมอและต้องยอมรับว่าเราไม่สามารถที่จะเลี่ยงได้เลย เช่น การถูกโจมตีด้วยแรมซัมแวร์ (Ransomware) ที่เกิดจากความเลินเล่อของพนักงานเอง การเกิดผลกระทบจากภัยธรรมชาติที่ไม่สามารถเลี่ยงได้ หรือ การเกิดเหตุจากปัจจัยภายนอกอย่างโรคระบาดหรือเหตุการณ์ไม่สงบทางการเมือง เป็นต้น การยอมรับเหตุที่จะเกิดขึ้นได้และมีแนวทางในการรับมือจึงเป็นแนวทางที่ดีที่สุดในการลดผลกระทบ ซึ่งหน่วยงานต้องมีความสามารถในการตอบสนองและกู้คืนระบบให้กลับมาทำงานได้อย่างต่อเนื่องและยืดหยุ่น หรือที่เรียกว่า Cyber Resilience ดังนั้น หากหน่วยงานมีการจัดทำแผนรับมือที่มีประสิทธิภาพ เมื่อเหตุภัยคุกคามดังกล่าว แผนการรับมือนี้ก็จะช่วยเป็นแนวทางให้หน่วยงานได้รับผลกระทบน้อยที่สุด และสามารถดำเนินภารกิจของตนเองไปได้อย่างต่อเนื่อง

แม้ว่าหลักการ Cyber Resilience จะเป็นแนวคิดใหม่ที่คำนึงถึงการตอบสนองต่อเหตุ แต่นั่นไม่ได้หมายความว่าหน่วยงานจะสามารถละเลยการป้องกันที่ดีเหมือนแต่ก่อนได้ โดยทั่วไป ในขั้นแรกหน่วยงานจะต้องมีการประเมินความเสี่ยงและป้องกันข้อมูลตามหลักการ CIA (Confidentiality - การรักษาความลับของข้อมูล, Integrity – ความถูกต้องครบถ้วนของข้อมูล, Availability - การคงสภาพความพร้อมการใช้งานข้อมูล) วิเคราะห์จุดอ่อนภายในระบบเพื่อติดตั้งระบบป้องกันที่เหมาะสม เช่น ไฟร์วอลล์ ซอฟต์แวร์ป้องกันไวรัส และระบบยืนยันตัวตน เพื่อให้ข้อมูลหน่วยงานมีความลับ ปลอดภัย และพร้อมใช้งานอยู่เสมอ

อีกแนวทางที่สำคัญที่เป็นการเตรียมความพร้อมในการตอบสนองต่อเหตุ คือการสำรองข้อมูล (Backup) อย่างสม่ำเสมอ ควรเลือกพื้นที่เก็บข้อมูลที่ปลอดภัย เพื่อให้สามารถกู้คืนข้อมูลได้อย่างรวดเร็วกรณีระบบถูกโจมตี นอกจากนี้ การทดสอบการกู้คืนข้อมูล (Recovery) เป็นประจำจะช่วยให้แน่ใจว่าระบบสามารถทำงานได้อย่างมีประสิทธิภาพ สุดท้ายนี้ หน่วยงานควรมีแผนรับมือและฟื้นฟู (Incident Response Plan) เมื่อเกิดเหตุการณ์โจมตีทางไซเบอร์ แผนนี้ควรระบุบทบาทหน้าที่ของทีมรับมือเหตุการณ์ (Incident Response Team) วิธีการหยุดยั้งการแพร่กระจายของภัยคุกคาม กระบวนการกู้คืนระบบ และแนวทางการสื่อสารกับผู้ที่

เกี่ยวข้องกับการที่มีแผนที่ชัดเจนจะช่วยให้หน่วยงานสามารถลดความเสียหายและฟื้นตัวได้อย่างรวดเร็ว ซึ่งสิ่งเหล่านี้เป็นไปตามหลักการของ Cyber Resilience

สิ่งที่จะช่วยในการปรับแนวคิดพนักงานให้เข้าใจแนวคิดของ Cyber Resilience ก็คือการสร้างความตระหนักรู้ด้านความปลอดภัยให้กับพนักงานทุกคน หน่วยงานควรจัดอบรมให้พนักงานมีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ วิธีป้องกันตัวเองเบื้องต้น การปฏิบัติตัวที่ปลอดภัยภายในระบบเครือข่าย และการตอบสนองต่อภัยคุกคามอย่างทันท่วงทีเมื่อเกิดเหตุและไม่เกิดความตระหนก

ทั้งนี้กรอบการทำงานของ Cyber Resilience จะเป็นไปตามเอกสาร NIST Special Publication 800-160, Volume 2 Revision 1 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach ซึ่งจะกล่าวในหัวข้อถัดไป ได้มีการแบ่งหัวข้อต่าง ๆ ได้แก่ การระบุความเสี่ยง (Identify) การป้องกันความเสี่ยง (Protect) การตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) การเผชิญเหตุภัยคุกคามภัยคุกคามทางไซเบอร์ (Respond) และการฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover) ซึ่งกรอบการทำงานนี้เสมือนเป็นมาตรการที่ครอบคลุม และสอดรับทันกับความเปลี่ยนแปลงต่าง ๆ รวมถึงภัยคุกคามที่เกิดขึ้น และมีการประเมินความเสี่ยงอย่างสม่ำเสมอ ซึ่งหากหน่วยงานมีการดำเนินการตามหลักการของ Cyber Resilience นี้แล้ว จะเป็นการช่วยให้หน่วยงานสามารถฟื้นตัวหลังจากการถูกโจมตีทางไซเบอร์และสามารถทำให้การดำเนินธุรกิจกลับคืนสู่สภาวะปกติได้อย่างรวดเร็ว

ตัวอย่างการเตรียมตัว และตอบสนองต่อภัยคุกคามทางไซเบอร์ (Cyber Resilience) มีดังนี้

- ร้านค้าปลีกออนไลน์ถูกโจมตีด้วย Ransomware ข้อมูลลูกค้า และสินค้าถูกเข้ารหัสจนไม่สามารถเข้าถึงได้ ผู้ดูแลระบบมีการสำรองข้อมูลไว้เป็นประจำ ทำให้สามารถกู้คืนข้อมูลได้อย่างรวดเร็ว และระบบสามารถกลับมาใช้งานได้ตามปกติ
- เว็บไซต์ของโรงพยาบาลถูกโจมตีด้วย (Distributed Denial-of-Service: DDoS) ซึ่งจะส่งผลให้ผู้ป่วยไม่สามารถนัดหมายแพทย์ออนไลน์ได้ ทีม IT ของโรงพยาบาลสามารถตรวจจับการโจมตีได้ทันที และมีระบบป้องกันที่จะช่วยลดผลกระทบ ทำให้เว็บไซต์ยังคงให้บริการได้บางส่วน
- พนักงานในบริษัทเผลอกดลิ้งค์ Phishing ทำให้มัลแวร์เข้าสู่ระบบคอมพิวเตอร์ของบริษัท บริษัทมีระบบตรวจจับและป้องกันภัยคุกคาม (Endpoint Detection and Response: EDR) ที่สามารถหยุดยั้งการแพร่กระจายของมัลแวร์ได้ทันที ช่วยให้ระบบไม่เกิดความเสียหายในวงกว้างและระบบสามารถกลับมาใช้งานได้ปกติ
- แฮกเกอร์กลุ่มหนึ่งสามารถเจาะเข้าสู่ฐานข้อมูลของธนาคารขนาดใหญ่ ขโมยข้อมูลส่วนตัวของลูกค้าจำนวนมาก ความเสียหายที่เกิดขึ้นไม่เพียงแค่ความเสียหายทางการเงิน แต่ยังส่งผลต่อความเชื่อมั่นของลูกค้าที่มีต่อธนาคารอีกด้วย ธนาคารแห่งนี้มีแผนรับมือเหตุการณ์ฉุกเฉินด้านไซเบอร์ที่รัดกุม รวมถึงการแจ้งเตือนลูกค้าที่ได้รับผลกระทบอย่างรวดเร็ว และมีมาตรการชดเชยเยียวยาที่เหมาะสม ธนาคารสามารถรักษาความเชื่อมั่นของลูกค้าไว้ได้ แม้จะมีเหตุการณ์โจมตีทางไซเบอร์เกิดขึ้น

- โรงไฟฟ้าแห่งหนึ่งถูกโจมตีไปที่ระบบควบคุมการผลิตไฟฟ้า ทำให้ส่งผลกระทบต่อการจ่ายกระแสไฟฟ้าเป็นวงกว้าง รวมถึงระบบสาธารณูปโภคอื่น ๆ ได้รับผลกระทบเป็นจำนวนมาก โรงไฟฟ้าแห่งนี้มีระบบตรวจจับ และป้องกันการบุกรุก (Intrusion Detection and Prevention System: IDS/IPS) ที่ทันสมัย สามารถระบุ และหยุดยั้งการโจมตีได้ทันที นอกจากนี้ยังมีระบบสำรองฉุกเฉิน (Redundancy) ที่ช่วยให้ระบบกลับมาจ่ายไฟฟ้าได้อย่างรวดเร็ว ช่วยลดความเสียหายที่อาจเกิดขึ้นต่อชีวิต และทรัพย์สิน
- ห้างสรรพสินค้าขนาดใหญ่ถูกโจมตีด้วย Ransomware ข้อมูลการขาย สต็อกสินค้า และข้อมูลลูกค้าถูกเข้ารหัส ผู้โจมตีเรียกร้องค่าไถ่เป็นจำนวนเงินมหาศาล ห้างสรรพสินค้าแห่งนี้มีการสำรองข้อมูลอย่างสม่ำเสมอ และมีแผนการรับมือ และตอบสนองที่มีประสิทธิภาพ รวมถึงมีแผนการสื่อสารกับผู้ได้รับผลกระทบ ทำให้สามารถกู้คืนข้อมูลได้อย่างรวดเร็ว ห้างสรรพสินค้าตัดสินใจไม่จ่ายค่าไถ่ และสามารถกลับมาเปิดดำเนินการได้ตามปกติภายในระยะเวลาอันสั้น เหตุการณ์นี้ส่งผลกระทบต่อภาพลักษณ์ของห้างสรรพสินค้าเพียงเล็กน้อย เนื่องจากมีความโปร่งใสในการสื่อสารกับลูกค้า

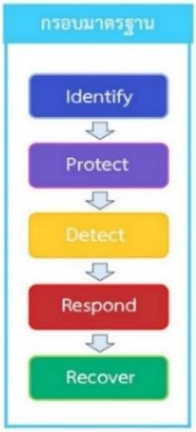
แนวทางปฏิบัติในการจัดทำแผนการรับมือจะถูกอธิบายโดยละเอียดในหัวข้อ 7.1 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

3. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework)

กรอบมาตรฐานการทำงานเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นแนวทางสำคัญช่วยปกป้องข้อมูล ทรัพย์สิน และชื่อเสียงของหน่วยงาน ซึ่งกรอบมาตรฐานนี้จะเป็นการสร้างแนวทางการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์แบบองค์รวม ไม่ว่าหน่วยงานมีขนาดเล็ก หรือใหญ่ก็ล้วนสามารถปรับไปใช้ได้ เพื่อให้สอดคล้องกับกฎระเบียบ ข้อบังคับต่าง ๆ ของหน่วยงานอีกด้วย กล่าวได้ว่า การนำกรอบมาตรฐานนี้มาประยุกต์ใช้ เปรียบเสมือนการสร้างเกราะป้องกันองค์กรจากภัยไซเบอร์อย่างรอบด้าน ช่วยให้หน่วยงานดำเนินภารกิจหลักไปได้ด้วยวิธีการแบบปลอดภัย กรอบมาตรฐานนี้ประยุกต์จาก NIST Cybersecurity Framework ซึ่งประกอบด้วย 5 หัวข้อหลัก ซึ่งจะกล่าวในหัวข้อถัดไป และกล่าวแยกโดยละเอียดในบทที่ 4 ถึงบทที่ 8

กรอบมาตรฐาน

ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 กรอบมาตรฐานประกอบไปด้วย 5 หัวข้อหลัก (ดังรูปที่ 1) ดังนี้



รูปที่ 1 กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

3.1. การระบุความเสี่ยง (Identify)

การระบุความเสี่ยงเป็นขั้นตอนแรกซึ่งเปรียบเสมือนการทำความรู้จักหน่วยงานของตัวเองอย่างละเอียด หน่วยงานจำเป็นต้องระบุระบบสารสนเทศ ข้อมูล ทรัพย์สิน และกระบวนการต่าง ๆ ที่มีอยู่ภายในรวมถึงประเมินความเสี่ยงด้านไซเบอร์เพื่อค้นหาจุดอ่อนที่อาจถูกโจมตีได้ การระบุเหล่านี้จะช่วยให้กำหนดเป้าหมาย ปรับแต่งมาตรการป้องกัน และวางแผนรับมือได้อย่างมีประสิทธิภาพ ในกรอบมาตรฐานได้อธิบายไว้ดังนี้

การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สิน และชีวิตร่างกายของบุคคล (Identify)

- *การจัดการทรัพย์สิน (Asset Management)*

- *การประเมินความเสี่ยง และกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)*
- *การประเมินช่องโหว่ และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)*
- *การจัดการผู้ให้บริการภายนอก (Third Party Management)*

3.2. การป้องกันความเสี่ยง (Protect)

เมื่อหน่วยงานทราบความเสี่ยงของตนเองแล้ว ขั้นตอนต่อไปจะเป็นการวางมาตรการการป้องกันเพื่อลดความเสี่ยง ตัวอย่างเช่น การตั้งค่าระบบรักษาความปลอดภัยให้แข็งแกร่ง การควบคุมการเข้าถึงข้อมูลอย่างเข้มงวด การติดตั้งระบบป้องกันไวรัสและมัลแวร์ การสร้างนโยบายความปลอดภัยที่ชัดเจน และการอบรมพนักงานให้มีความรู้และทักษะในการรับมือกับภัยคุกคามทางไซเบอร์ ในกรอบมาตรฐานได้อธิบายไว้ดังนี้

มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

- *การควบคุมการเข้าถึง (Access Control)*
- *การทำให้ระบบมีความแข็งแกร่ง (System Hardening)*
- *การเชื่อมต่อระยะไกล (Remote Connection)*
- *สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)*
- *การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)*
- *การแบ่งปันข้อมูล (Information Sharing)*

3.3. การตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

ขั้นตอนนี้กล่าวถึงการมีระบบตรวจสอบและเฝ้าระวังความผิดปกติ ซึ่งเปรียบเสมือนการติดตั้งกล้องวงจรปิดภายในหน่วยงาน ระบบเหล่านี้ เช่น (Security Information and Event Management: SIEM) และเครื่องมือสแกนช่องโหว่ เครื่องมือเหล่านี้จะช่วยให้สามารถระบุสัญญาณเตือนภัยของเหตุการณ์ด้านไซเบอร์ได้อย่างทันท่วงที เช่น การเข้าถึงระบบที่ผิดปกติ การแพร่กระจายของมัลแวร์ หรือพฤติกรรมที่น่าสงสัยอื่น ๆ ในกรอบมาตรฐานได้อธิบายไว้ดังนี้

มาตรการตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

- *การตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)*

3.4. การเผชิญเหตุภัยคุกคามภัยคุกคามทางไซเบอร์ (Respond)

เมื่อมีการตรวจสอบพบเหตุการณ์ภัยคุกคาม หน่วยงานต้องมีแผนการรับมือที่ชัดเจน และรวดเร็ว แผนนี้จะครอบคลุมกระบวนการต่าง ๆ เช่น การระบุ สอบสวน ควบคุมสถานการณ์ กำจัดภัยคุกคาม และลดผลกระทบ โดยมีเป้าหมายเพื่อหยุดยั้งการแพร่กระจายของภัย ปกป้องข้อมูลสำคัญ และฟื้นฟูระบบให้กลับมาใช้งานได้โดยเร็วที่สุด ในกรอบมาตรฐานได้อธิบายไว้ดังนี้

มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

- *แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)*
- *แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)*
- *การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)*

3.5. การฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover)

หลังจากผ่านพ้นเหตุการณ์ภัยคุกคาม การฟื้นฟูระบบ และข้อมูลถือเป็นสิ่งสำคัญ หน่วยงานควรมีแผนสำรองข้อมูล (Backup) ที่อัพเดตอยู่เสมอ เพื่อให้สามารถกู้คืนข้อมูลที่สูญหายได้อย่างรวดเร็ว นอกจากนี้ยังต้องมีกระบวนการตรวจสอบ และปรับปรุงระบบรักษาความปลอดภัย เพื่อป้องกันไม่ให้เหตุการณ์ลักษณะเดียวกันเกิดขึ้นอีก ในกรอบมาตรฐานได้อธิบายไว้ดังนี้

มาตรการรักษา และฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

- *การรักษา และฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)*

4. การระบุความเสี่ยง (Identify)

การระบุความเสี่ยง (Identify) มีความสำคัญในการบริหารจัดการความเสี่ยงด้านไซเบอร์ โดยหน่วยงานจำเป็นจะต้องรู้จักตนเอง ตั้งแต่ วัตถุประสงค์ เป้าหมาย ทรัพย์สิน ข้อมูล และผลกระทบที่เกิดขึ้นหากสิ่งข้างต้นไม่เป็นไปตามที่คาดหวัง ส่วนที่เป็นทรัพย์สิน รวมถึงข้อมูล เป็นสิ่งที่ยิ่งต้องปกป้อง ดังนั้นหน่วยงานจึงต้องประเมินความเสี่ยงว่าแต่ละทรัพย์สิน หรือข้อมูล มีโอกาสถูกโจมตีมากน้อยเพียงใด ผลกระทบหากถูกโจมตีรุนแรงเพียงใด การระบุ และประเมินความเสี่ยงอย่างชัดเจน ช่วยให้กระบวนการอื่น ได้แก่ ป้องกัน (Protect) ตรวจจับ (Detect) ตอบสนอง (Respond) และฟื้นฟู (Recover) ในขั้นตอนถัดไปมีประสิทธิภาพ มุ่งเน้นไปยังจุดที่อ่อนแอ สร้างเกราะป้องกันได้ตรงจุด

4.1. การจัดการทรัพย์สิน (Asset Management)

กรอบมาตรฐาน

1) ต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน ในการระบุทรัพย์สินนั้นต้องคำนึงถึงปัจจัยเหล่านี้

- ระบุทรัพย์สินที่เกี่ยวข้องกับข้อมูลสารสนเทศของหน่วยงาน
- เป็นทรัพย์สินสารสนเทศที่ส่งผลกระทบกระบวนการทำงาน และผลประกอบการของหน่วยงานในส่วนของ Confidentiality (การรักษาความลับของข้อมูล) Integrity (การรักษาความสมบูรณ์ของข้อมูล) และ Availability (การรักษาสภาพพร้อมใช้งานของข้อมูล)
- ไม่จำเป็นต้องระบุ หากทรัพย์สินนั้นไม่เกี่ยวข้องกับข้อมูลสารสนเทศของหน่วยงาน หรือเกี่ยวข้องแต่ไม่มีความสำคัญ หรือส่งผลกระทบใด ๆ ต่อหน่วยงาน

โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

(ก) *ชื่อ/คำอธิบายของทรัพย์สิน ของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ*

(ข) *ฟังก์ชันที่สำคัญของทรัพย์สิน ของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ*

(ค) *การระบุ และการจัดลำดับความสำคัญของทรัพย์สิน บริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ*

(ง) *เจ้าของ และ/ หรือผู้ดำเนินการของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ*

(จ) *ตำแหน่งทางกายภาพของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแต่ละรายการ*

(ฉ) *การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศบนระบบ/เครือข่ายภายใน และ/ หรือภายนอก*

2) ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรง และมีนัยสำคัญ (Direct and Significant Interface)

- ระบุขอบเขตให้ชัดเจนในส่วนของเครือข่าย และระบบที่เชื่อมต่อกับทรัพย์สินที่มีความสำคัญ หรือส่งผลกระทบต่อหน่วยงาน
- วิเคราะห์ผลกระทบว่าหากระบบ หรือเครือข่ายเกิดความเสียหาย หรือหยุดทำงานในระยะเวลาหนึ่ง แล้วส่งผลกระทบต่อหน่วยงาน หรือไม่ ซึ่งการวิเคราะห์ผลกระทบนี้จะช่วยในการกำหนดขอบเขตได้ดีเพราะหากไม่ส่งผลกระทบใด ๆ แสดงว่าไม่อยู่ในขอบเขต

3) ต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ 1 (หนึ่ง) ครั้ง ทั้งนี้การกำหนดกรอบเวลา 1 ครั้งต่อปี เป็นเพียงข้อแนะนำขั้นต่ำ หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย ซึ่งหากมีการเปลี่ยนแปลงดังต่อไปนี้ ควรจะมีการตรวจสอบทะเบียนทรัพย์สินอีกครั้ง

- การเปลี่ยนแปลงระบบสารสนเทศในหน่วยงาน เช่น ติดตั้งระบบใหม่ รื้อถอนระบบเดิม (Decommission) เปลี่ยนแปลงโครงสร้างระบบเครือข่าย เป็นต้น
- การเปลี่ยนแปลงด้านบุคลากร รวมถึงโครงสร้างหน่วยงาน และตำแหน่งงาน ซึ่งส่งผลต่อสิทธิในการเข้าถึง และการกำหนดผู้รับผิดชอบ
- การเกิดภัยคุกคามในรูปแบบใหม่ เมื่อได้รับข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ในรูปแบบใหม่ที่กำลังระบาด หรือเมื่อหน่วยงานเพิ่งผ่านพ้นเหตุภัยคุกคามไซเบอร์ ควรที่จะมีการทบทวนทะเบียนทรัพย์สินอีกครั้ง เพื่อเตรียมความพร้อม และป้องกัน
- การเปลี่ยนแปลงในกฎ ระเบียบ และนโยบาย ซึ่งอาจจะมีการเปลี่ยนแปลงในข้อบังคับในการจัดทำทะเบียนทรัพย์สิน จึงจำเป็นจะต้องทบทวนอีกครั้งว่าข้อมูลในทะเบียนทรัพย์สินในปัจจุบันเป็นไปตามข้อบังคับใหม่ทางกฎหมาย หรือไม่

4) ตามมาตรา 54 ของ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 กำหนดให้ต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์สินในข้อ 1 อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง

- การประเมินความเสี่ยงควรกระทำควบคู่ไปกับการตรวจสอบทะเบียนทรัพย์สิน เพื่อที่จะได้ทราบว่าหากทรัพย์สินใด (รวมถึงระบบสารสนเทศ และข้อมูล) ถูกโจมตีทางไซเบอร์ หน่วยงานจะได้รับผลกระทบมากน้อยเพียงใด ซึ่งการประเมินความเสี่ยงในรูปแบบนี้ จะเป็นการประเมินโดยอิงตามทรัพย์สินเป็นที่ตั้ง
- การกำหนดกรอบเวลาข้างต้น เป็นเพียงข้อแนะนำขั้นต่ำ หากเกิดการเปลี่ยนแปลงใด ๆ ในข้อที่กล่าวมาข้างต้น หน่วยงานจะต้องประเมินความเสี่ยงอีกครั้ง (รายละเอียดอยู่ในบทถัดไป)

5) *การจัดทำทะเบียนทรัพย์สิน สามารถทำในรูปแบบอย่างง่ายลงในตาราง* ตัวอย่างการจัดทำทะเบียนทรัพย์สิน ได้ถูกแสดงด้านล่างนี้

ทะเบียนทรัพย์สินประเภทฮาร์ดแวร์

เลขทะเบียนทรัพย์สินสารสนเทศ	Serial Number	รายการ	ผู้รับผิดชอบ	ที่ตั้ง	ระบบ	กลุ่มทรัพย์สิน
HW-001	SN000001	Router AAA รุ่น BBB	IT	ห้อง Data Center อาคาร 1	โครงสร้างพื้นฐานสารสนเทศ	Router
HW-002	SN000002	Firewall AAA รุ่น BBB	IT	ห้อง Data Center อาคาร 1	โครงสร้างพื้นฐานสารสนเทศ	Firewall
HW-003	SN000003	Switch AAA รุ่น BBB	IT	ห้อง Data Center อาคาร 1	โครงสร้างพื้นฐานสารสนเทศ	Switch
HW-004	SN000004	Server AAA รุ่น BBB	IT	ห้อง Data Center อาคาร 1	โครงสร้างพื้นฐานสารสนเทศ	Server
HW-005	SN000005	Storage AAA รุ่น BBB	IT	ห้อง Data Center อาคาร 1	โครงสร้างพื้นฐานสารสนเทศ	Storage

ทะเบียนทรัพย์สินประเภทซอฟต์แวร์

เลขทะเบียนทรัพย์สินสารสนเทศ	รายการ	ผู้รับผิดชอบ	จัดเก็บอยู่ที่	ระบบ	กลุ่มทรัพย์สิน
SW-001	Windows Server 2022	IT	ห้อง Data Center อาคาร 1	โครงสร้างพื้นฐานสารสนเทศ	OS Group 1
SW-002	Windows 11 Pro	IT	ห้อง Data Center อาคาร 1	โครงสร้างพื้นฐานสารสนเทศ	OS Group 2
SW-003	Linux Mint 21.3	IT	ห้อง Data Center อาคาร 1	โครงสร้างพื้นฐานสารสนเทศ	OS Group 3
SW-004	Antivirus	IT	ห้อง Data Center อาคาร 1	โครงสร้างพื้นฐานสารสนเทศ	Antivirus
SW-005	Network Monitoring	IT	ห้อง Data Center อาคาร 1	โครงสร้างพื้นฐานสารสนเทศ	Network Monitor
SW-006	Backup Management	IT	ห้อง Data Center อาคาร 1	โครงสร้างพื้นฐานสารสนเทศ	Backup

ทะเบียนทรัพย์สินประเภทข้อมูล

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อข้อมูล/สารสนเทศ	รายละเอียดข้อมูล/สารสนเทศ	ระดับชั้นความลับ	สื่อบันทึก / สถานที่จัดเก็บ	ผู้รับผิดชอบ	กลุ่มทรัพย์สิน
INFO-001	Network diagram	ข้อมูลแผนภาพโครงสร้างพื้นฐานระบบเครือข่าย	Confidential	File Server / ห้อง Data Center อาคาร 1	IT	Network diagram
INFO-002	Network log file	ข้อมูลบันทึกกิจกรรมต่าง ๆ ภายในระบบ	Confidential	File Server /	IT	Network log file

เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อข้อมูล/สารสนเทศ	รายละเอียดข้อมูล/สารสนเทศ	ระดับชั้นความลับ	สื่อบันทึก / สถานที่จัดเก็บ	ผู้รับผิดชอบ	กลุ่มทรัพย์สิน
				ห้อง Data Center อาคาร 1		
INFO-003	Source Code	โค้ดของระบบ	Internal Use	File Server / ห้อง Data Center อาคาร 1	IT	Source Code
INFO-004	Data Backup	เป็นข้อมูลสำรองของระบบงานสารสนเทศ	Confidential	NAS Storage / ห้อง Data Center อาคาร 1	IT	Backup file
INFO-005	Network Configuration	ข้อมูลการ Config Network	Confidential	File Server / ห้อง Data Center อาคาร 1	IT	Network Configuration

ตารางที่ 2 แบบประเมินตนเองด้านการจัดการทรัพย์สิน (Asset Management)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้น ซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. หน่วยงานมีการจัดทำทะเบียนทรัพย์สิน หรือไม่		
2. หน่วยงานมีการทบทวนทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง หรือไม่		
3. หน่วยงานมีการทบทวนทะเบียนทรัพย์สินเมื่อมีการเปลี่ยนแปลงระบบสารสนเทศ หรือไม่		
4. หน่วยงานมีการทบทวนทะเบียนทรัพย์สินเมื่อมีการเปลี่ยนแปลงด้านบุคลากร หรือไม่		
5. หน่วยงานมีการทบทวนทะเบียนทรัพย์สินเมื่อได้รับข่าวภัยคุกคามทางไซเบอร์รูปแบบใหม่ หรือที่กำลังระบาด หรือเมื่อหน่วยงานเพิ่งผ่านพ้นภัยคุกคามไซเบอร์ หรือไม่		
6. หน่วยงานมีการทบทวนทะเบียนทรัพย์สินเมื่อมีการเปลี่ยนแปลงทางด้านกฎหมาย หรือไม่		
7. หน่วยงานมีการสื่อสารในเรื่องการจัดทำทะเบียนทรัพย์สินไปยังผู้มีส่วนได้เสียภายในหน่วยงาน หรือไม่		

4.2. การประเมินความเสี่ยง และกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

เนื่องจากภัยคุกคามทางไซเบอร์สามารถมุ่งเป้าไปที่ Confidentiality (การรักษาความลับของข้อมูล), Integrity (การรักษาความสมบูรณ์ของข้อมูล) และ Availability (การรักษาสภาพพร้อมใช้งานของข้อมูล) ทำให้ผลกระทบดังกล่าวจะส่งผลให้เกิดความเสียหายทั้งด้านชีวิต ด้านทรัพย์สิน ด้านสังคม ด้านภาพลักษณ์ขององค์กร รวมไปถึงการส่งผลต่อกฎหมายตัวอื่น ๆ อีก เช่น พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎหมายลำดับรองที่เกี่ยวข้องด้วย

กรอบมาตรฐาน

1) ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการประกาศกำหนด การเปลี่ยนแปลงที่สำคัญดังกล่าว ประกอบไปด้วย

- การเปลี่ยนแปลงระบบสารสนเทศในหน่วยงาน เช่น ติดตั้งระบบใหม่ รื้อถอนระบบเดิม (Decommission) เปลี่ยนแปลงโครงสร้างระบบเครือข่าย เป็นต้น
- การเปลี่ยนแปลงด้านบุคลากร รวมถึงโครงสร้างหน่วยงาน และตำแหน่งงาน ซึ่งส่งผลต่อสิทธิในการเข้าถึง และการกำหนดผู้รับผิดชอบ
- การเกิดภัยคุกคามในรูปแบบใหม่ เมื่อได้รับข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ในรูปแบบใหม่ที่กำลังระบาด หรือเมื่อหน่วยงานเพิ่งผ่านพ้นเหตุภัยคุกคามไซเบอร์ ควรที่จะมีการประเมินความเสี่ยงอีกครั้ง
- การเปลี่ยนแปลงในกฎ ระเบียบ และนโยบาย ซึ่งอาจจะส่งผลต่อระดับความเสี่ยงที่มากขึ้น หรือน้อยลง จึงจำเป็นที่จะต้องประเมินความเสี่ยงอีกครั้ง
- การเปลี่ยนแปลงสภาพแวดล้อมทางธุรกิจ (Business Environment) ซึ่งเป็นการเปลี่ยนแปลงภาวะแวดล้อมที่ธุรกิจไม่สามารถควบคุมได้ เช่น การเมือง เศรษฐกิจ โรคระบาด เป็นต้น
- การเปลี่ยนแปลงกลยุทธ์ของหน่วยงาน รวมถึงการเปลี่ยนแปลงทางวิสัยทัศน์ พันธกิจ หรือการเปลี่ยนแปลงรูปแบบการให้บริการ หรือกลุ่มลูกค้า หรือผู้มีส่วนได้เสีย
- การเปลี่ยนแปลงในเรื่องงบประมาณ และทรัพยากร ซึ่งจะส่งผลต่อความสามารถในการบริหารจัดการความเสี่ยงที่มีอยู่

2) ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสารโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) *วันที่ระบุความเสี่ยง (Date the Risk is Identified)*

(ข) *คำอธิบายของความเสี่ยง (Description of the Risk)*

(ค) *โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)*

(ง) *ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)*

(จ) *การจัดการความเสี่ยง (Risk Treatment)*

(ฉ) *เจ้าของความเสี่ยง (Risk Owner)*

(ช) *สถานะของการจัดการความเสี่ยง (Status of Risk Treatment) และ*

(ซ) *ความเสี่ยงที่เหลือ (Residual Risk)*

ตัวอย่างด้านล่างนี้เป็นเพียงแนวทางการดำเนินงาน หน่วยงานต้องนำไปปรับเพื่อให้เหมาะสมและสอดคล้องกับเกณฑ์ระดับความสำคัญของหน่วยงาน

ตัวอย่าง การประเมินความเสี่ยงมีดังนี้

ตัวอย่าง เกณฑ์ระดับผลกระทบของความเสี่ยง (Consequence Level)	
ระดับความรุนแรง	คำจำกัดความของแต่ละระดับ
สูงมาก (5)	– กระทบต่อภาพลักษณ์ และชื่อเสียงของหน่วยงานอย่างมีสาระสำคัญ – เกิดความสูญเสียต่อระบบสารสนเทศที่สำคัญ และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่าง ๆ (> 500,000 บาท)
สูง (4)	เกิดปัญหาต่อระบบสารสนเทศที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อ ความถูกต้องของข้อมูลบางส่วน (100,000 - 500,000 บาท)
ปานกลาง (3)	ระบบสารสนเทศมีปัญหา และมีความสูญเสียไม่มาก (50,000 - 100,000 บาท)
น้อย (2)	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้ (5,000 - 50,000 บาท)
น้อยมาก (1)	– ไม่กระทบต่อภาพลักษณ์ และชื่อเสียงของหน่วยงาน – เกิดเหตุร้ายที่ไม่มีความสำคัญ (< 5,000 บาท)

ตัวอย่าง เกณฑ์ระดับโอกาสของการเกิดความเสี่ยง (Likelihood Level)		
ระดับโอกาสเกิดความเสี่ยง	โอกาสที่จะเกิด	โอกาส/ความถี่
สูงมาก (5)	มีโอกาสเกิดเหตุการณ์มากกว่า 90% ภายในระยะเวลา 12 เดือนข้างหน้า	เกือบทุกวัน

ตัวอย่าง เกณฑ์ระดับโอกาสของการเกิดความเสี่ยง (Likelihood Level)		
ระดับโอกาสเกิดความเสี่ยง	โอกาสที่จะเกิด	โอกาส/ความถี่
สูง (4)	มีโอกาสเกิดมากกว่า 50% แต่ไม่เกิน 90% ภายในระยะเวลา 12 เดือนข้างหน้า	วันเว้นวัน
ปานกลาง (3)	มีโอกาสเกิดมากกว่า 25% แต่ไม่เกิน 50% ภายในระยะเวลา 12 เดือนข้างหน้า	สัปดาห์ละ 2 ครั้ง
น้อย (2)	มีโอกาสเกิดมากกว่า 5% แต่ไม่เกิน 25% ภายในระยะเวลา 12 เดือนข้างหน้า	สัปดาห์ละ 1 ครั้ง
น้อยมาก (1)	มีโอกาสเกิดเหตุการณ์น้อยกว่า หรือเท่ากับ 5% ภายในระยะเวลา 12 เดือนข้างหน้า	เดือนละ 1 ครั้ง

ตัวอย่างการกำหนดเกณฑ์ และการคำนวณระดับความเสี่ยง

ระดับความเสี่ยง (Risk Level) = โอกาสของการเกิด (Likelihood) x ผลกระทบ (Consequence)

Risk Matrix		ผลกระทบของความเสี่ยง (Consequence)				
		น้อยมาก (1)	น้อย (2)	ปานกลาง (3)	สูง (4)	สูงมาก (5)
โอกาสของการเกิดความเสี่ยง (Likelihood)	สูงมาก (5)	ปานกลาง (5)	สูง (10)	สูงมาก (15)	สูงมาก (20)	สูงมาก (25)
	สูง (4)	ปานกลาง (4)	ปานกลาง (8)	สูง (12)	สูงมาก (16)	สูงมาก (20)
	ปานกลาง (3)	ต่ำ (3)	ปานกลาง (6)	สูง (9)	สูง (12)	สูงมาก (15)
	น้อย (2)	ต่ำ (2)	ปานกลาง (4)	ปานกลาง (6)	ปานกลาง (8)	สูง (10)
	น้อยมาก (1)	ต่ำ (1)	ต่ำ (2)	ต่ำ (3)	ปานกลาง (4)	ปานกลาง (5)

ตัวอย่าง ระดับความเสี่ยง (Risk Level)	
ระดับความเสี่ยง	**ความหมาย**
สีแดง **สูงมาก (Very High)**	เป็นความเสี่ยงที่ส่งผลกระทบอย่างรุนแรง จำเป็นต้องจัดการอย่างเร่งด่วน พร้อมทั้งดำเนินการจัดทำแผนจัดการความเสี่ยงเพื่อลดระดับความเสี่ยง และป้องกันไม่ให้เกิดความเสี่ยงในระดับที่สูงขึ้น
สีส้ม **สูง (High)**	เป็นความเสี่ยงที่ส่งผลกระทบสูง จำเป็นต้องจัดการโดยเร็ว พร้อมทั้งดำเนินการจัดทำแผนจัดการความเสี่ยงเพื่อลดระดับความเสี่ยง และป้องกันไม่ให้เกิดความเสี่ยงในระดับที่สูงขึ้น
สีเหลือง **ปานกลาง (Medium)**	เป็นความเสี่ยงที่ส่งผลกระทบปานกลาง จำเป็นต้องจัดการถัดจากระดับความเสี่ยงสีแดง และสีส้ม พร้อมทั้งดำเนินการจัดทำแผนจัดการความเสี่ยงเพื่อลดระดับความเสี่ยง และป้องกันไม่ให้เกิดความเสี่ยงในระดับที่สูงขึ้น
สีเขียว **ต่ำ (Low)**	เป็นความเสี่ยงที่ยอมรับได้ มีแนวทางในการควบคุมความเสี่ยง และเฝ้าระวังความเสี่ยงอย่างสม่ำเสมอ

การประเมินความเสี่ยงประเภทฮาร์ดแวร์

Asset Type	Asset Group	Threat	Vulnerability	Existing Control	Risk Analysis					
					Consequence Level			Consequence	Likelihood	Risk Level
					C	I	A			
Hardware โครงสร้างพื้นฐานสารสนเทศ	Access Point	ทรัพย์สินสูญหาย	ขาดการจัดทำทะเบียนทรัพย์สิน	มีการจัดทำทะเบียนทรัพย์สิน และมีการบริหารจัดการทรัพย์สิน รวมถึงจะดำเนินการทบทวนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง	Yes	Yes	Yes	3	1	3
Hardware โครงสร้างพื้นฐานสารสนเทศ	Core Switch	ถูกเข้าถึงโดยไม่ได้รับอนุญาต	ขาดการกำหนดสิทธิระดับสิทธิในการเข้าถึงระบบสารสนเทศ	มีการกำหนดสิทธิระดับสิทธิในการเข้าถึงระบบสารสนเทศ โดยบริหารจัดการการเข้าถึงระบบสารสนเทศด้วยระบบ AD ทั้งนี้ยังมีการทบทวนสิทธิอย่างน้อยปีละ 1 ครั้ง	Yes	Yes	Yes	3	1	3
Hardware โครงสร้างพื้นฐานสารสนเทศ	Firewall	ถูกเข้าถึงโดยไม่ได้รับอนุญาต	ขาดการป้องกันการเข้าถึงอุปกรณ์สารสนเทศที่ไม่มีผู้ดูแลประจำ	มีการกำหนดนโยบายทรัพย์สินกรณีที่ไม่มีการดูแล และมีการตรวจเช็คทรัพย์สิน	Yes	Yes	Yes	3	1	3
Hardware โครงสร้างพื้นฐานสารสนเทศ	Server	ทรัพย์สินชำรุดเสียหาย	ขาดการออกแบบและติดตั้งอุปกรณ์	มีการออกแบบ และติดตั้งอุปกรณ์ให้มีความมั่นคงปลอดภัย	No	Yes	Yes	3	1	3

Asset Type	Asset Group	Threat	Vulnerability	Existing Control	Risk Analysis					
					Consequence Level			Consequence	Likelihood	Risk Level
					C	I	A			
			ให้มีความมั่นคงปลอดภัย	ซึ่งรวมถึงการเดินสายสัญญาอย่างมั่นคงปลอดภัย						
Hardware โครงสร้างพื้นฐานสารสนเทศ	Storage	อุปกรณ์ไม่พร้อมใช้งาน	ขาดการบำรุงรักษาอุปกรณ์	มีการ MA อุปกรณ์ที่สนับสนุนของกองทุนฯ และตรวจสอบความพร้อมใช้งานของอุปกรณ์อย่างสม่ำเสมอ	No	No	Yes	3	1	3

ตัวอย่าง การประเมินความเสี่ยงประเภทซอฟต์แวร์

Asset Type	Asset Group	Threat	Vulnerability	Existing Control	Risk Analysis					
					Consequence Level			Consequence	Likelihood	Risk Level
					C	I	A			
Software ในระบบโครงสร้างพื้นฐานสารสนเทศ	ซอฟต์แวร์ระบบป้องกันไวรัส (Antivirus)	ระบบถูกบุกรุก	ขาดการติดตามข้อมูลข่าวสารด้านภัยคุกคาม	– มีการตั้งไลน์กลุ่มไว้สำหรับแลกเปลี่ยนข้อมูลที่มีความสนใจพิเศษในเรื่องเดียวกัน รวมไปถึงมีการกดติดตามข้อมูลข่าวสารทางไซเบอร์ตาม	Yes	No	No	2	2	4

Asset Type	Asset Group	Threat	Vulnerability	Existing Control	Risk Analysis					
					Consequence Level			Consequence	Likelihood	Risk Level
					C	I	A			
				ช่องทางต่าง ๆ เช่น Website, Facebook เป็นต้น – มีการวิเคราะห์ข้อมูลภัยคุกคามเชิงลึก – ไม่อนุญาตให้เจ้าหน้าที่เข้าเว็บไซต์ที่เป็นอันตราย หรือสุ่มเสี่ยง พร้อมทั้งมีการกำหนดนโยบายที่เกี่ยวข้องการการเข้าถึงเว็บไซต์อย่างมั่นคงปลอดภัยไว้เป็นลายลักษณ์อักษร						
Software ในระบบโครงสร้างพื้นฐานสารสนเทศ	ซอฟต์แวร์ระบบศูนย์คอมพิวเตอร์สำรอง	ข้อมูลรั่วไหล	ขาดการควบคุมการเข้าถึงซอร์สโค้ด	มีการควบคุมการเข้าถึงซอร์สโค้ดโดยผู้ที่มีสิทธิเข้าถึงซอร์สโค้ดได้คือผู้พัฒนาระบบเท่านั้น	Yes	No	No	2	1	2
Software ในระบบโครงสร้างพื้นฐานสารสนเทศ	ซอฟต์แวร์ระบบศูนย์คอมพิวเตอร์สำรอง	ระบบล่ม	ขาดระเบียบข้อบังคับในการสำรองข้อมูลสารสนเทศ	มีการสำรองข้อมูลสารสนเทศพร้อมทั้งทดสอบการกู้คืนข้อมูลสารสนเทศ	No	Yes	Yes	3	1	3

Asset Type	Asset Group	Threat	Vulnerability	Existing Control	Risk Analysis					
					Consequence Level			Consequence	Likelihood	Risk Level
					C	I	A			
Software ในระบบโครงสร้างพื้นฐานสารสนเทศ	ระบบเฝ้าดู และแจ้งเตือนอัตโนมัติ (Environment Monitoring System)	ระบบถูกบุกรุก	ขาดการติดตามข้อมูลข่าวสารด้านภัยคุกคาม	– มีการตั้งไลน์กลุ่มไว้สำหรับแลกเปลี่ยนข้อมูลที่มีความสนใจพิเศษในเรื่องเดียวกัน รวมไปถึงมีการกดติดตามข้อมูลข่าวสารทางไซเบอร์ตามช่องทางต่าง ๆ เช่น Website, Facebook เป็นต้น – มีการวิเคราะห์ข้อมูลภัยคุกคามเชิงลึก – ไม่อนุญาตให้เจ้าหน้าที่เข้าเว็บไซต์ที่เป็นอันตราย หรือสุ่มเสี่ยง พร้อมทั้งมีการกำหนดนโยบายที่เกี่ยวข้องการการเข้าถึงเว็บไซต์อย่างมั่นคงปลอดภัยไว้เป็นลายลักษณ์อักษร	Yes	No	No	2	2	4

Asset Type	Asset Group	Threat	Vulnerability	Existing Control	Risk Analysis					
					Consequence Level			Consequence	Likelihood	Risk Level
					C	I	A			
Software ในระบบโครงสร้างพื้นฐานสารสนเทศ	ระบบ Privileged Access Management	ระบบถูกโจมตี	ขาดการติดตามข้อมูลข่าวสารด้านภัยคุกคาม	– มีการตั้งไลน์กลุ่มไว้สำหรับแลกเปลี่ยนข้อมูลที่มีความสนใจพิเศษในเรื่องเดียวกัน รวมไปถึงมีการกดติดตามข้อมูลข่าวสารทางไซเบอร์ตามช่องทางต่าง ๆ เช่น Website, Facebook เป็นต้น – มีการวิเคราะห์ข้อมูลภัยคุกคามเชิงลึก – ไม่อนุญาตให้เจ้าหน้าที่เข้าเว็บไซต์ที่เป็นอันตราย หรือสุ่มเสี่ยง พร้อมทั้งมีการกำหนดนโยบายที่เกี่ยวข้องการการเข้าถึงเว็บไซต์อย่างมั่นคงปลอดภัยไว้เป็นลายลักษณ์อักษร	Yes	Yes	Yes	3	2	6

ตัวอย่าง การประเมินความเสี่ยงประเภทข้อมูล

Asset Type	Asset Group	Threat	Vulnerability	Existing Control	Risk Analysis					
					Consequence Level			Consequence	Likelihood	Risk Level
					C	I	A			
Information	Network diagram	ข้อมูลรั่วไหล	ขาดการกำหนดนโยบาย และขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ	มีการกำหนดนโยบาย และขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการบริหารจัดการเครือข่ายอย่างมั่นคงปลอดภัย	Yes	No	No	2	1	2
Information	Network log file	ข้อมูลรั่วไหล	ขาดการเข้ารหัสข้อมูลที่สำคัญ	มีการกำหนดนโยบายเข้ารหัสข้อมูล ทั้งนี้ข้อมูลที่สำคัญจะมีการเข้ารหัสข้อมูล โดยจะเข้ารหัสข้อมูลด้วยวอัลกอริทึมที่กำหนดไว้	Yes	No	No	2	1	2
Information	Source Code	ข้อมูลไม่พร้อมใช้งาน	ขาดการสำรองข้อมูลสารสนเทศ	มีการสำรองข้อมูลสารสนเทศพร้อมทั้งทดสอบการกู้คืนข้อมูลสารสนเทศ	No	Yes	Yes	3	1	3

Asset Type	Asset Group	Threat	Vulnerability	Existing Control	Risk Analysis					
					Consequence Level			Consequence	Likelihood	Risk Level
					C	I	A			
Information	Network Config	ข้อมูลถูกแก้ไขโดยไม่ได้รับอนุญาต	ขาดการจำกัดการเข้าถึงข้อมูลสารสนเทศ	มีการจำกัดการเข้าถึงข้อมูลสารสนเทศ โดยกำหนดสิทธิระดับสิทธิในการเข้าถึงระบบสารสนเทศให้เข้าถึงได้เฉพาะที่อนุญาตให้เข้าถึง โดยบริหารจัดการการเข้าถึงระบบสารสนเทศด้วยระบบ AD ทั้งนี้ยังมีการทบทวนสิทธิอย่างน้อยปีละ 1 ครั้ง	Yes	Yes	Yes	3	1	3
Information	CCTV DATA	ถูกเข้าถึงโดยไม่ได้รับอนุญาต	ขาดการบริหารจัดการสื่อบันทึกข้อมูล	มีบริหารจัดการสื่อบันทึกข้อมูลโดยกำหนดไว้เป็นนโยบายในการจัดการสื่อบันทึกข้อมูล รวมไปถึงกรณีที่มีการใช้งานสื่อบันทึกข้อมูลจะต้องขออนุญาตก่อนการใช้งาน	Yes	No	No	3	1	3

ตัวอย่าง การประเมินความเสี่ยงของบุคลากร

Asset Type	Asset Group	Threat	Vulnerability	Existing Control	Risk Analysis					
					Consequence Level			Consequence	Likelihood	Risk Level
					C	I	A			
People	ผู้อำนวยการฝ่าย	ทำผิดกฎหมายระเบียบข้อบังคับ	ไม่มีการประกาศนโยบายฯ ให้รับทราบทั่วกัน	มีประกาศนโยบายตามภาครัฐเพื่อให้หน่วยงานภาครัฐปฏิบัติตาม รวมไปถึงนโยบายที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยเพื่อเป็นแนวทางให้กับเจ้าหน้าที่เกี่ยวข้องปฏิบัติตามนโยบายที่กำหนดไว้	Yes	Yes	Yes	2	1	2
People	ผู้อำนวยการฝ่าย	ทำผิดกฎหมายระเบียบข้อบังคับ	ขาดกระบวนการพิจารณาโทษทางวินัย	มีกระบวนการลงโทษทางวินัยของกองทุนฯ ไว้ในระเบียบคู่มือของพนักงาน	Yes	Yes	Yes	2	1	2
People	หัวหน้ากลุ่มงาน	ทำผิดกฎหมายระเบียบข้อบังคับ	ขาดการชี้แจงข้อตกลง และเงื่อนไขในการจ้างงาน	มีการชี้แจงข้อตกลงเงื่อนไขในการจ้างงานไว้เป็นลายลักษณ์อักษร	Yes	Yes	Yes	2	1	2

Asset Type	Asset Group	Threat	Vulnerability	Existing Control	Risk Analysis					
					Consequence Level			Consequence	Likelihood	Risk Level
					C	I	A			
People	หัวหน้ากลุ่มงาน	ถูกสวมสิทธิในการเข้าถึงระบบสารสนเทศ	ไม่มีการป้องกันข้อมูลลับในการพิสูจน์ตัวตนในการเข้าใช้งานระบบอย่างเหมาะสม	พนักงานมี AD ช่วยในการบริหารจัดการให้มีความมั่นคงปลอดภัย รวมไปถึงการมีการกำหนดสิทธิในการเข้าถึงระบบสารสนเทศไว้ใน Access rights matrix	Yes	Yes	Yes	2	1	2
People	เจ้าหน้าที่	ทำงานผิดพลาด	ขาดคู่มือ ขั้นตอนการปฏิบัติงานในการทำงานกับระบบสารสนเทศ	มีคู่มือการปฏิบัติงานต่าง ๆ ที่เกี่ยวข้องในฝ่ายเทคโนโลยีสารสนเทศ	No	Yes	Yes	3	1	3

ตารางที่ 3 แบบประเมินตนเองด้านการประเมินความเสี่ยง และกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้น ซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. หน่วยงานมีการประเมินความเสี่ยง หรือไม่		
2. หน่วยงานมีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง หรือไม่		
3. หน่วยงานมีการทบทวนการประเมินความเสี่ยงเมื่อมีการเปลี่ยนแปลงระบบสารสนเทศ หรือไม่		
4. หน่วยงานมีการทบทวนการประเมินความเสี่ยงเมื่อมีการเปลี่ยนแปลงด้านบุคลากร หรือไม่		
5. หน่วยงานมีการทบทวนการประเมินความเสี่ยงเมื่อได้รับข่าวภัยคุกคามทางไซเบอร์รูปแบบใหม่ หรือที่กำลังระบาด หรือเมื่อหน่วยงานเพิ่งผ่านพ้นภัยคุกคามไซเบอร์ หรือไม่		
6. หน่วยงานมีการทบทวนการประเมินความเสี่ยงเมื่อมีการเปลี่ยนแปลงทางด้านกฎหมาย หรือไม่		
7. หน่วยงานมีการทบทวนการประเมินความเสี่ยงเมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมทางธุรกิจ (Business Environment) หรือไม่		
8. หน่วยงานมีการทบทวนการประเมินความเสี่ยงเมื่อมีการเปลี่ยนแปลงกลยุทธ์ของหน่วยงาน หรือไม่		
9. หน่วยงานมีการทบทวนการประเมินความเสี่ยงเมื่อมีการเปลี่ยนแปลงในเรื่องงบประมาณ และทรัพยากร หรือไม่		
10. หน่วยงานมีการสื่อสารในเรื่องการประเมินความเสี่ยงไปยังผู้มีส่วนได้เสียทั้งภายในหน่วยงาน และภายนอกหน่วยงาน หรือไม่		

4.3. การประเมินช่องโหว่ และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

กรอบมาตรฐาน

1) ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญ ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงานเพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัย และการควบคุมโดยครอบคลุมบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งเป็น

(ก) *ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) system)*

- ระบบสารสนเทศที่ใช้ในสำนักงานอย่าง Web Application, Email Server, ระบบเครือข่ายในสำนักงาน เป็นต้น

(ข) *ระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System: ICS)*

- ระบบต่าง ๆ โรงงานอุตสาหกรรม เช่น Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLCs), อุปกรณ์ Operational Technology (OT) เป็นต้น

2) ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

(ก) *การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)*

(ข) *การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)*

(ค) *การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)*

(ง) *ซึ่งการประเมินความมั่นคงปลอดภัยดังกล่าว สามารถแยกรายละเอียดดังต่อไปนี้*

- ประเมินช่องโหว่ของโฮสต์ เช่น การตรวจสอบเวอร์ชันของซอฟต์แวร์และการติดตั้ง Patch ที่เหมาะสม การตรวจสอบการตั้งค่า เป็นต้น
- ประเมินช่องโหว่ในส่วนของซอฟต์แวร์ด้วยวิธีที่เป็นที่ยอมรับ เช่น ตรวจสอบช่องโหว่ของ Web Application อ้างอิงตาม OWASP Top 10
- จัดการ Patch คือ ตรวจสอบ Security Patch ว่าเหมาะสม หรือไม่ มีการทดสอบ Patch ก่อนติดตั้ง และมีการอัพเดตสม่ำเสมอ หรือไม่
- ตรวจสอบการตั้งค่าว่าเป็นไปตามนโยบายความมั่นคงปลอดภัย และมาตรฐานที่เหมาะสม หรือไม่
- ติดตั้งโปรแกรม Antivirus หรือ Anti-malware และอัพเดตอย่างสม่ำเสมอ หรือไม่
- ตรวจสอบสิทธิการเข้าถึงระบบ
- มีการจัดเก็บข้อมูล Log และบริหารจัดการข้อมูล Log ที่เหมาะสม

- ตรวจสอบ Network Topology เพื่อเข้าใจสถาปัตยกรรมในภาพรวม และอุปกรณ์หรือระบบที่เกี่ยวข้อง
- ตรวจสอบการตั้งค่าระบบความมั่นคงปลอดภัยของเครือข่าย เช่น Firewall, การควบคุมการเข้าถึงระบบเครือข่าย
- ตรวจสอบการเข้ารหัสลับข้อมูลทั้งข้อมูลระหว่างที่เดินทาง และเมื่ออยู่ในที่จัดเก็บ
- ตรวจสอบระบบยืนยันตัวบุคคล และควบคุมการเข้าถึง ว่ามีความถูกต้องในระดับที่ยอมรับได้ หรือไม่
- ตรวจสอบความพร้อมในการตอบสนองต่อภัยคุกคาม (Incident Response)
- ตรวจสอบความมั่นคงปลอดภัยทางกายภาพ
- ตรวจสอบว่าระดับความมั่นคงปลอดภัยของข้อมูลเป็นไปตามกฎหมายที่เกี่ยวข้องหรือไม่ เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นต้น
- วิเคราะห์ประเภทของข้อมูลด้วยว่าเป็นข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) หรือข้อมูลที่ไม่ใช่ข้อมูลส่วนบุคคล รวมถึงระดับชั้นความลับกรณีที่ไม่ใช่ข้อมูลส่วนบุคคล เช่น รหัสผ่าน หรือความลับทางการค้า เป็นต้น ซึ่งข้อมูลแต่ละประเภทจะต้องมีระดับความเข้มข้นในการรักษาความมั่นคงปลอดภัยที่แตกต่างกัน
- รับทราบบทบาทของตนเองว่าเป็นผู้ควบคุมข้อมูล (Data Controller) หรือผู้ประมวลผลข้อมูล (Data Processor) และมีการดำเนินที่เหมาะสมตามบทบาทของตนเอง และไม่ว่าจะอยู่ในบทบาทใด หากผู้ควบคุมข้อมูลต้องใช้บริการหน่วยงานภายนอกซึ่งเป็นผู้ประมวลผลข้อมูล ในเรื่องของการประมวลผลข้อมูลส่วนบุคคล ทั้งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจำเป็นจะต้องมีข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) สามารถอ่านรายละเอียดได้ที่ https://www.pdpc.or.th/2797/

3) ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัย และควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญ ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

- กำหนดขอบเขตการทดสอบ และประเมินให้ชัดเจน
- ทำการทดสอบ และประเมินอย่างครอบคลุม และถี่ถ้วนทั้งการทดสอบตามฟังก์ชันว่าทำงานถูกต้องหรือไม่ (Functional Testing) และการทดสอบนอกเหนือจากการทดสอบฟังก์ชันพื้นฐาน (Non-Functional Testing) เช่น Performance Stress Test, Scalability Test, Reliability Test เป็นต้น

- แจ้งผู้ที่เกี่ยวข้องที่อาจได้รับผลกระทบ เช่น ผู้ใช้บริการ โฮสต์ผู้ให้บริการคลาวด์แก่หน่วยงานที่เป็นเจ้าของระบบ เป็นต้น
- ควรมีการทดสอบ และประเมินช่องโหว่ตั้งแต่ในระยะแรกของการพัฒนาระบบ ไปตลอดช่วงวงจรการพัฒนาระบบ เช่น การรีวิวโค้ด (Code Review) และ การเขียนโค้ดให้ปลอดภัย (Secure Coding) เป็นต้น
- ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบ หรือความเสี่ยงจากการทดสอบเจาะระบบด้วย ในการทดสอบเจาะระบบ มีแนวทางการเตรียมความพร้อมคล้ายคลึงกับการประเมินช่องโหว่ข้างต้น แต่มีส่วนที่เพิ่มเติมคือควรบันทึกขอบเขตและรายละเอียดการทดสอบเป็นเอกสารให้ชัดเจน เพื่อใช้ในการตรวจสอบว่าการทดสอบนั้นไม่ขัดต่อนโยบาย กฎ ระเบียบ และมาตรฐานทางจริยธรรม
- วางแผนการตอบสนองต่อเหตุไม่พึงประสงค์ เนื่องจากการทดสอบอาจส่งผลกระทบ หรือความเสียหายที่ไม่พึงประสงค์
- สำรองข้อมูล และมีวิธีในการกู้คืนข้อมูลได้อย่างเหมาะสม
- ในระหว่างการทดสอบ หมั่นตรวจตราระบบอย่างสม่ำเสมอถึงเหตุไม่พึงประสงค์ที่อาจเกิดขึ้น และมีความพร้อมในการตอบสนองต่อเหตุดังกล่าว

4) ต้องตรวจสอบให้แน่ใจถึงขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยเฉพาะอย่างยิ่ง ทุกระบบที่เป็นมีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

- กำหนดขอบเขตให้ละเอียด เช่น IP Address, ระบบ, ฟังก์ชัน เป็นต้น
- กำหนดขอบเขตส่วนที่จะทดสอบ และส่วนที่ไม่ทดสอบที่จะต้องไม่ได้รับผลกระทบจากการทดสอบนั้น
- วิเคราะห์ว่าการทดสอบนี้ครอบคลุมข้อกำหนดทางกฎหมาย มาตรฐานอุตสาหกรรม หรือความต้องการของลูกค้า หรือผู้ใช้บริการ หรือไม่

5) ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 (หนึ่ง) ครั้ง ตามความจำเป็นเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

6) ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบ และผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรอง และได้รับ

ประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ ทั้งนี้คุณสมบัติของผู้ทดสอบเจาะระบบให้เป็นไปตามหลักเกณฑ์ และวิธีการที่หน่วยงานควบคุม หรือกำกับดูแลกำหนด

- พิจารณาเลือกผู้ทดสอบเจาะระบบตามวัตถุประสงค์ของการทดสอบ เช่น หากทดสอบเพื่อวัตถุประสงค์ภายในหน่วยงาน สามารถเลือกผู้ทดสอบภายในหน่วยงานเอง หรือจากภายนอกหน่วยงาน แต่หากทดสอบเพื่อสร้างความเชื่อมั่นแก่ลูกค้า หรือผู้ใช้บริการภายนอก ควรเลือกผู้ทดสอบจากภายนอกหน่วยงาน เป็นต้น

- ผู้ทดสอบระบบไม่ว่าจะมาจากหน่วยงานเดียวกัน หรือจากภายนอกหน่วยงาน จะต้องเป็นอิสระจากระบบที่ทำการทดสอบ เช่น ผู้ทดสอบไม่ได้มีส่วนร่วมในการพัฒนาระบบที่ต้องการทดสอบ เป็นต้น

- ผู้ทดสอบระบบจะต้องมีความรู้ ความสามารถ ในการเจาะระบบโดยเฉพาะ หากหน่วยงานไม่มีบุคลากรที่มีคุณสมบัติเพียงพอ ควรใช้บริการผู้ทดสอบจากภายนอก เพื่อหลีกเลี่ยงผลการทดสอบที่ผิดพลาด และไม่ครอบคลุม รวมถึงหลีกเลี่ยงการทดสอบที่ไม่เป็นไปตามหลักธรรมาภิบาล เช่น กรณีที่หน่วยงานมีบุคลากรไม่เพียงพอ จึงใช้บุคลากรที่อยู่ในทีมพัฒนาระบบเดียวกันเป็นผู้ทดสอบเอง

7) ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของหน่วยงาน

8) ต้องสร้างกระบวนการเพื่อติดตาม และจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบ และตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

- ภายหลังจากการประเมินช่องโหว่และทดสอบเจาะระบบ จำเป็นจะต้องวิเคราะห์ผลการประเมินหรือทดสอบให้ถี่ถ้วนถึงผลกระทบหากไม่ได้รับการแก้ไข หากวิเคราะห์แล้วมีความเสี่ยงหรือจะเกิดความเสียหาย จะต้องทำการแก้ไขจนอยู่ในระดับที่สามารถยอมรับได้ แต่หากวิเคราะห์แล้วพบว่าไม่มีความเสี่ยง ความเสี่ยงที่ต่ำมาก หรือจะไม่เกิดความเสียหายใดๆ สามารถพิจารณาที่จะยอมรับความเสี่ยงนั้นได้

9) หากได้รับการร้องขอ (ตามกฎหมาย) จากคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) หรือ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบเพื่อประโยชน์ในการประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานดังกล่าว ไปยังสำนักงานภายในกำหนด 30 (สามสิบ) วัน นับแต่วันที่ได้รับหนังสือด้วย ทั้งนี้ รูปแบบรายงานสรุปผลการทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์ และวิธีการที่สำนักงานประกาศกำหนด

- หน่วยงานต้องศึกษากฎหมายที่เกี่ยวข้องเกี่ยวกับการรายงานสรุปผลการทดสอบเจาะระบบ หรือรายงานด้านความมั่นคงปลอดภัยไซเบอร์อื่น ๆ ที่เป็นประโยชน์ ไปยังหน่วยงานกำกับที่เกี่ยวข้องภายในระยะเวลาที่กำหนด

- หน่วยงานจำเป็นจะต้องจัดทำรายงานเอกสารดังกล่าวอย่างเป็นประจำ และต้องเตรียมพร้อมเพื่อใช้เป็นหลักฐานในการดำเนินการด้วยวิธีแบบปลอดภัย ทั้งนี้แนวปฏิบัติในการดำเนินการ

ดังกล่าว หน่วยงานยังสามารถใช้เป็นแนวทางในการดูแล และกำกับด้านความมั่นคงปลอดภัยไซเบอร์แก่ผู้รับจ้างด้วย ในกรณีที่หน่วยงานเป็นผู้ว่าจ้างในการพัฒนาระบบ

ตารางที่ 4 แบบประเมินตนเองด้านการประเมินช่องโหว่ และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้น ซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. หน่วยงานมีการทดสอบประเมินเป็นประจำ หรือไม่		
2. หน่วยงานมีการทดสอบเจาะระบบเป็นประจำ หรือไม่		
3. หน่วยงานมีความเข้าใจถึงความแตกต่างระหว่างการทดสอบประเมิน และการทดสอบเจาะระบบ หรือไม่		
4. หน่วยงานมีการจัดทำเอกสารรายงานการทดสอบดังกล่าว หรือไม่		
5. หน่วยงานมีบุคลากรภายในสำหรับการทดสอบดังกล่าว หรือไม่		
6. หน่วยงานมีแผน หรือกำหนดการในการดำเนินการทดสอบดังกล่าว หรือไม่		
7. หน่วยงานมีแนวทางในการรายงานผลการทดสอบดังกล่าว ไปยังหน่วยงานภายนอกเมื่อถูกร้องขอ หรือไม่		

4.4. การจัดการผู้ให้บริการภายนอก (Third Party Management)

กรอบมาตรฐาน

1) ต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แม้ว่าผู้ให้บริการภายนอกจะดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- คัดเลือกผู้ให้บริการภายนอกที่มีคุณสมบัติที่เหมาะสม
- กำหนดขอบเขต หน้าที่ความรับผิดชอบ ให้ชัดเจน
- กำหนดให้ผู้รับจ้างต้องปฏิบัติตามนโยบาย แนวปฏิบัติของหน่วยงานในการให้บริการอย่างเคร่งครัด ทั้งในส่วนของการรักษาความมั่นคงปลอดภัย การคุ้มครองข้อมูลส่วนบุคคล ธรรมาภิบาลข้อมูล และส่วนอื่น ๆ ที่เกี่ยวข้อง และต้องระบุใน Term of Reference (TOR)

2) ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) *ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามความต้องการทางธุรกิจขององค์กร และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์*

(ข) *ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจากภัยคุกคามทางไซเบอร์*

(ค) *ความเสี่ยงที่เกี่ยวข้องกับบริการ และห่วงโซ่อุปทานผลิตภัณฑ์*

(ง) *สิทธิ์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก*

นอกจากนี้ ในการกำหนด SLA จำเป็นที่จะต้องคำนึงถึงสิ่งเหล่านี้ด้วย

- ให้มองว่า SLA เป็นข้อตกลงการให้บริการหรือเสมือนเป็นสัญญาการให้บริการ ซึ่งหากการให้บริการผิดไปจากที่กำหนดไว้ใน SLA จะต้องระบุให้ชัดว่าผู้ให้บริการจะต้องมีการชดใช้อะไรบ้าง
- กำหนด SLA ที่สอดคล้องกับประสิทธิภาพการทำงาน ความมั่นคงปลอดภัย และความเป็นส่วนตัว การคุ้มครองข้อมูลส่วนบุคคล
- กำหนด SLA ที่สามารถวัดผลได้ เช่น เวลาในการตอบสนอง เปอร์เซ็นต์ในสภาพที่พร้อมใช้ (Availability Percentages) เวลาในการแก้ปัญหาหลังเกิดเหตุ เป็นต้น การกำหนด SLA ที่ชัดเจน และวัดผลได้นี้ จะเป็นประโยชน์ทั้ง 2 ฝ่ายระหว่างหน่วยงานว่าจ้าง และหน่วยงานภายนอกซึ่งเป็นผู้รับจ้าง
- กำหนด SLA ที่สอดคล้องกับกลยุทธ์ และเป้าหมายของหน่วยงาน

- กำหนด SLA ที่สอดคล้องกับข้อกำหนดทางกฎหมาย และกฎระเบียบ และนโยบายของหน่วยงาน
- เปิดช่องให้ SLA สามารถยืดหยุ่นตามความต้องการในการเปลี่ยนแปลงต่าง ๆ ในหน่วยงานได้
- กำหนดบทลงโทษ หรือวิธีชดเชยหากหน่วยงานภายนอกให้บริการในระดับที่ต่ำกว่าที่กำหนดใน SLA

3) ควรพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สามและการตรวจสอบผลิตภัณฑ์

- ตรวจประเมินผู้ให้บริการภายนอกโดยผู้ตรวจประเมินที่อิสระ และไม่มีส่วนได้เสียกับผู้ให้บริการภายนอก
- กำกับดูแลการทำงานของผู้ให้บริการภายนอกอย่างสม่ำเสมอตลอดช่วงที่ให้บริการ เช่น การรีวิวข้อมูล Logs การตรวจรายงานของผู้ให้บริการภายนอก เป็นต้น
- มีการจัดประชุมกับผู้ให้บริการภายนอกเป็นระยะ เพื่อประเมินระดับคุณภาพการให้บริการ
- กำหนดคุณสมบัติให้ผู้ให้บริการภายนอก (หรือผลิตภัณฑ์ที่ผู้ให้บริการภายนอกใช้) ได้รับการรับรอง หรือมีประกาศนียบัตรที่ได้รับการยอมรับในบริการที่เกี่ยวข้อง

4) ควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมาย หรือข้อบังคับใหม่

- สัญญาจ้าง หรือ SLA ต้องมีความยืดหยุ่น เพื่อรองรับการเปลี่ยนแปลงทางกฎหมายและระเบียบภายในของหน่วยงาน
- นอกจากการเปลี่ยนแปลงทางกฎหมายแล้ว ยังรวมถึงการเปลี่ยนแปลงอื่น ๆ ภายในหน่วยงาน เช่น ความต้องการทางธุรกิจ เทคโนโลยีที่ใช้ เป็นต้น
- ในเรื่องของการคุ้มครองข้อมูลส่วนบุคคล หน่วยงานต้องรับทราบบทบาทของตนเองว่าเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หรือผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) และมีการดำเนินการที่เหมาะสมตามบทบาทของตนเอง และไม่ว่าจะอยู่ในบทบาทใด หากผู้ควบคุมข้อมูลส่วนบุคคลต้องใช้บริการหน่วยงานภายนอกซึ่งเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจำเป็นจะต้องมีข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) สามารถอ่านรายละเอียดได้ที่ https://www.pdpc.or.th/2797/

ตัวอย่าง การกำหนด SLA

เช่น ระดับการให้บริการ (SLA) ของผู้ให้บริการระบบเครือข่าย (Network System) ที่ร้อยละ 95

<u>เงื่อนไขการให้บริการ</u>

บริการแบบ 24 ชั่วโมง X 7 วันต่อสัปดาห์

<u>วิธีการวัด</u>

$$\frac{\text{(ระยะเวลาให้บริการในรอบที่ทำการวัด - ระยะเวลาที่เกิด Down Time) X 100}}{\text{ระยะเวลาให้บริการในรอบที่ทำการวัด}}$$

<u>ผู้รับผิดชอบ</u>

ฝ่ายเทคโนโลยีสารสนเทศ

<u>ความถี่ในการวัด</u>

ทุกไตรมาส (3 เดือน)

หมายเหตุ : ประมาณเวลาระยะเวลาที่ไม่สามารถให้บริการ (Down Time) เมื่อกำหนดระดับการให้บริการที่ร้อยละ 95 (SLA 95%)

- 1 เดือน ระยะเวลาที่ไม่สามารถให้บริการต้องไม่เกิน 8 ชั่วโมง
- 1 ไตรมาส (3 เดือน) ระยะเวลาที่ไม่สามารถให้บริการต้องไม่เกิน 24 ชั่วโมง
- 1 ปี ระยะเวลาที่ไม่สามารถให้บริการต้องไม่เกิน 96 ชั่วโมง

ตารางที่ 5 แบบประเมินตนเองด้านการจัดการผู้ให้บริการภายนอก (Third Party Management)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้นซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. หน่วยงานมีการกำหนด SLA แก่ผู้ให้บริการภายนอก หรือไม่		
2. SLA เป็นไปตามความต้องการของหน่วยงาน และตามข้อบังคับทางกฎหมาย หรือไม่		
3. หน่วยงานมีกระบวนการในการตรวจประเมินผู้ให้บริการภายนอก หรือไม่		
4. หน่วยงานมีกระบวนการกำกับ ดูแล และติดตามการดำเนินงานของผู้ให้บริการภายนอกว่าการดำเนินงานเป็นไปตาม SLA หรือไม่		
5. หน่วยงานมีการกำหนดบทลงโทษ หรือวิธีชดเชย ในกรณีที่ผู้ให้บริการภายนอกไม่ดำเนินการตาม SLA หรือไม่		
6. หน่วยงานมีการกำหนดคุณสมบัติว่าผู้ให้บริการภายนอกจะต้องมีใบรับรอง หรือประกาศนียบัตรที่ได้รับการยอมรับ หรือไม่		
7. หน่วยงานมีการประชุมกับผู้ให้บริการภายนอกเพื่อประเมินผลการให้บริการเป็นระยะ หรือไม่		

5. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

มาตรการป้องกัน (Protect) ถือเป็นหนึ่งในมาตรการที่สำคัญที่สุดในขั้นตอนด้านความมั่นคงปลอดภัยไซเบอร์ การสร้าง และใช้มาตรการป้องกันที่เหมาะสมจะช่วยลด หรือจำกัดผลกระทบจากเหตุการณ์ด้านไซเบอร์ที่อาจเกิดขึ้น โดยอาศัยการทำงานร่วมกับกระบวนการต่าง ๆ เช่น การควบคุมการเข้าถึง การติดตั้งโปรแกรมด้านการป้องกันภัยไซเบอร์ และอัพเดตอย่างสม่ำเสมอ การสร้างนโยบาย และกระบวนการรักษาความปลอดภัยที่มั่นคง การสร้างความตระหนัก และฝึกอบรมบุคลากร เป็นต้น ดังนั้น การป้องกัน คือหัวใจสำคัญในการลดความเสี่ยงทางไซเบอร์ ซึ่งมีค่าใช้จ่ายที่น้อยกว่าการแก้ไข อย่างมาก

5.1. การควบคุมการเข้าถึง (Access Control)

ขั้นตอนปฏิบัติ

1. ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศถูกจำกัดไว้ที่

(ก) *บุคลากร และกิจกรรมที่ได้รับอนุญาต และ*

(ข) *อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต*

โดยมีรายละเอียดดังนี้

- กำหนดให้ชัดเจนว่าใคร หรือกลุ่มผู้ใช้งานใดมีสิทธิในการเข้าถึงระบบ หรือข้อมูลใดบ้าง หรือใช้วิธีกำหนดสิทธิอื่น ๆ ที่เหมาะสม
- จัดทำเกณฑ์การกำหนดสิทธิในระดับบุคคล กลุ่มบุคคล หรือระดับอื่น ๆ และขั้นตอนในการกำหนดสิทธิ เปลี่ยนแปลงสิทธิ และการยกเลิกสิทธิ
- ในระบบที่มีความสำคัญสูง ให้พิจารณาใช้การกำหนดสิทธิแบบ Role-Based Access Control (RBAC) ซึ่งเป็นการกำหนดสิทธิจากบทบาท หรือตำแหน่งแทนที่จะระบุไปที่ตัวบุคคล
- การใช้วิธีการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) มาใช้เพื่อเพิ่มระดับความมั่นคงปลอดภัย แต่ต้องพิจารณาถึงความสะดวกในการใช้งานควบคู่กันไปด้วย
- ตรวจสอบข้อมูล Log จากการเข้าถึงข้อมูล และการทำธุรกรรมต่าง ๆ อย่างสม่ำเสมอ
- พิจารณาทำการแบ่งส่วนเครือข่าย (Network Segmentation) เพื่อแยกข้อมูลที่มีความอ่อนไหว ข้อมูลที่มีชั้นความลับสูง เพื่อความสะดวกต่อการควบคุมการเข้าถึงเฉพาะกลุ่มที่มีสิทธิ รวมถึงพิจารณาใช้ Firewall และมาตรการความมั่นคงปลอดภัยทางเครือข่ายอื่น ๆ ร่วมกัน
- พิจารณามาตรการการควบคุมอุปกรณ์ในการเข้าถึงระบบ และข้อมูลของหน่วยงานด้วย เช่น ควบคุมการใช้อุปกรณ์ Bring Your Own Device (BYOD) อย่างโทรศัพท์มือถือ หรือแท็ปเล็ต ในการเข้าถึงเครือข่ายของหน่วยงาน หรือข้อมูลของหน่วยงาน เป็นต้น
- ต้องตรวจสอบความถูกต้องของสิทธิ และการควบคุมดังกล่าวอย่างสม่ำเสมอ หรือทุกครั้งเมื่อมีการเปลี่ยนแปลงระบบ หรือโครงสร้างของหน่วยงาน หรือบุคลากร

2. ในส่วนที่เกี่ยวกับภาระหน้าที่ภายใต้ข้อ 1. หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดให้แต่ละบุคลากร กิจกรรม และกระบวนการที่ได้รับอนุญาตมีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละวิธีการเข้าถึงบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- ควรมีการบันทึกทุกครั้งที่มีการกำหนดสิทธิ เปลี่ยนแปลงสิทธิ และการยกเลิกสิทธิ
- การกำหนดสิทธิในการเข้าถึงที่น้อยที่สุด หรือการกำหนดสิทธิเท่าที่จำเป็น (Least Privilege) ซึ่งการกำหนดสิทธิในระดับต่ำไว้ก่อนเป็นสิ่งพื้นฐานที่พึงกระทำ
- สื่อสาร หรือจัดอบรมในการสร้างความตระหนักในเรื่องของการเข้าถึงข้อมูล ความเสี่ยงที่เกิดขึ้น และนโยบาย หรือกฎหมายที่เกี่ยวข้อง

3. ต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และตรวจสอบบันทึกเหล่านี้ เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

- ใช้เครื่องมือในการบันทึกข้อมูล Log ที่เหมาะสม และบันทึกข้อมูล Log ที่จำเป็นให้ครบ เช่น ผู้ใช้งาน การเข้าถึงข้อมูล หรือระบบ และธุรกรรม หรือกิจกรรมใด ๆ ที่กระทำต่อข้อมูล หรือระบบ
- บันทึก Metadata ที่เกี่ยวข้องด้วย เช่น Timestamps, ชื่อบัญชีผู้ใช้งาน และประเภทของข้อมูล หรือระบบ เป็นต้น
- บริหารจัดการ Log ที่ส่วนกลาง (Centralized Log Management) เพื่อช่วยให้การตรวจสอบ และการวิเคราะห์ข้อมูลเป็นไปอย่างมีประสิทธิภาพ เช่น ช่วยให้ผู้ดูแลระบบสามารถรวบรวมข้อมูล Log จากระบบต่าง ๆ ที่หลากหลาย เพื่อวิเคราะห์ และสร้างรูปแบบ (Pattern) ของความผิดปกติได้ อันนำไปสู่การสืบสวน ป้องกัน และแก้ไขในอนาคตได้
- มีระบบการตรวจสอบ Log แบบ Real-Time
- มีระบบที่สามารถแจ้งเตือนความผิดปกติโดยอัตโนมัติ และมีขั้นตอนในการตอบสนองต่อเหตุดังกล่าวได้อย่างทันท่วงที
- มีการวิเคราะห์ความผิดปกติจากพฤติกรรมผู้ใช้งาน (Behavioral Analytics)
- ตรวจสอบกระบวนการบันทึกข้อมูล Log เกณฑ์ของเหตุการณ์ที่ผิดปกติ และเกณฑ์การแจ้งเตือน อย่างสม่ำเสมอ เพื่อตรวจสอบความสอดคล้องกับนโยบายของหน่วยงาน และกฎหมายที่เกี่ยวข้อง

4. ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดย

(ก) *ทำภายใต้การดูแลของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเท่านั้น และ*

(ข) *ดำเนินการในสถานที่ หากเป็นไปได้* (เฉพาะ Onsite หรือสถานที่ ที่กำหนด)

โดยมีรายละเอียดดังนี้

- ควรจัดทำนโยบายการเข้าถึงอินเทอร์เฟซเป็นลายลักษณ์อักษรโดยละเอียด และเข้าใจง่ายโดยผู้ใช้งานทุกกลุ่ม
- ใช้มาตรการการควบคุมทางเทคนิค เพื่อควบคุมการเข้าถึงอินเทอร์เฟซที่มีประสิทธิภาพมากขึ้น
- ศึกษานโยบายของหน่วยงานตนเอง และกฎหมายที่เกี่ยวข้อง รวมถึงข้อกำหนดขั้นต่ำด้านการรักษาความมั่นคงปลอดภัย หากต้องดำเนินการร่วมกับหน่วยงานของรัฐ หรือหน่วยงานโครงสร้างพื้นฐานที่เกี่ยวข้อง รวมถึงหน่วยงานที่กำกับดูแล
- หากหน่วยงานตนเองมีเกณฑ์ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยที่อยู่ในระดับสูงกว่าข้อกำหนดขั้นต่ำที่กำหนดโดยหน่วยงานที่กำกับดูแลให้ยึดตามข้อกำหนดของหน่วยงานตนเองเป็นหลัก

ตารางที่ 6 แบบประเมินตนเองด้านการควบคุมการเข้าถึง (Access Control)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้น ซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. หน่วยงานมีนโยบายควบคุมการเข้าถึงข้อมูล และได้สื่อสารแก่พนักงานทุกคน หรือไม่		
2. หน่วยงานมีการกำหนดสิทธิการเข้าถึงที่น้อยที่สุด หรือเท่าที่จำเป็น (Least Privilege) หรือไม่		
3. หน่วยงานมีการกำหนดสิทธิแบบ Role-Based Access Control (RBAC) หรือไม่		
4. หน่วยงานมีวิธีการยืนยันตัวตนแบบหลายปัจจัย (Multi-factor Authentication) หรือไม่		
5. หน่วยงานมีการบันทึกข้อมูล Log ในทุก ๆ การเข้าถึงข้อมูล หรือระบบ หรือไม่		
6. หน่วยงานมีระบบการบันทึก Log จากส่วนกลาง และมีการวิเคราะห์ และแจ้งเตือนแบบ Real Time หรือไม่		
7. หน่วยงานมีการตรวจสอบสิทธิการเข้าถึงของพนักงานทุกคนเป็นประจำ หรือไม่		
8. หน่วยงานมีขั้นตอนการยกเลิกสิทธิการเข้าถึงเมื่อผู้ใช้งานนั้นมีการเปลี่ยนตำแหน่งหรือหน้าที่ความรับผิดชอบ ซึ่งทำให้พนักงานต้องไม่สามารถเข้าถึงข้อมูลนั้นอีกต่อไป หรือไม่		
9. หน่วยงานมีการแบ่งส่วนเครือข่าย (Network Segmentation) และ Firewall เพื่อควบคุมการเข้าถึงข้อมูลสำคัญโดยเฉพาะ หรือไม่		
10. หน่วยงานมีขั้นตอนในการตอบสนองต่อเหตุการณ์ผิดปกติโดยทันท่วงที หรือไม่		

5.2. การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

ขั้นตอนปฏิบัติ

1. ต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- ควรจัดทำเอกสารมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ให้ละเอียด และสมบูรณ์ รวมถึงการกำหนดการตั้งค่าแบบปลอดภัย โดยอ้างอิงตามมาตรฐานอุตสาหกรรม คำแนะนำจากเจ้าของผลิตภัณฑ์ หรือผู้ให้บริการ และข้อกำหนดเฉพาะของหน่วยงาน และกฎหมายที่เกี่ยวข้อง
- เอกสารดังกล่าวควรกำหนดมาตรฐานในระดับที่ไม่ต่ำกว่ามาตรฐานที่ได้รับการยอมรับ เช่น ISO/IEC 27001, NIST Cybersecurity Framework หรือข้อกำหนดที่สามารถเทียบเคียงกับหน่วยงานหรือภาคอุตสาหกรรมที่เชื่อถือได้ (Benchmarking) เป็นต้น
- ตรวจสอบเอกสารดังกล่าวอย่างสม่ำเสมอเพื่อดูว่ายังคงสอดคล้องกับนโยบาย หรือกฎหมายที่เกี่ยวข้อง หรือความต้องการของหน่วยงาน หรือไม่
- จัดทำเอกสารดังกล่าวให้สอดคล้องกับแผนการตอบสนองต่อภัยคุกคาม
- มีการตรวจสอบช่องโหว่ของระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ อย่างสม่ำเสมอ

2. มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

1) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

- กำหนดสิทธิให้น้อยที่สุดเท่าที่จำเป็นโดยพิจารณาจากหน้าที่ความรับผิดชอบ
- พิจารณาใช้วิธีการควบคุมการเข้าถึงแบบ Role-based Access Control (RBAC)
- ตรวจสอบสิทธิการเข้าถึงอย่างสม่ำเสมอ

2) การแบ่งแยกหน้าที่ (Separation of Duties)

- แยกหน้าที่ หรือสิทธิการดำเนินการที่สำคัญบางอย่าง โดยไม่ให้กระทำโดยคนเพียงคนเดียว เพื่อป้องกันไม่ให้คน ๆ เดียวมีสิทธิที่มากเกินไป ซึ่งจะส่งผลในเรื่องของผลประโยชน์ทับซ้อน ความไม่มีธรรมาภิบาล และการทุจริต ตัวอย่างเช่น การแบ่งแยกหน้าที่ระหว่างผู้ดูแลระบบเครือข่าย และผู้ตรวจสอบช่องโหว่ของระบบเครือข่ายเดียวกัน เป็นต้น

3) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

- กำหนดนโยบายรหัสผ่านให้มีความซับซ้อน ซึ่งข้อกำหนดประกอบไปด้วยความยาวและประเภทของอักขระ
- พิจารณาการยืนยันตัวตนด้วยหลายปัจจัย (Multi-Factor Authentication) หากมีความจำเป็น และต้องพิจารณาถึงความสะดวกของผู้ใช้งานเป็นสำคัญด้วย

4) การลบบัญชีที่ไม่ได้ใช้

- ตรวจสอบบัญชีผู้ใช้งานอย่างสม่ำเสมอ ซึ่งรวมถึงบัญชีที่ไม่มีผู้ใช้งานแล้ว (เช่น พนักงานที่ลาออก) และบัญชีที่มีความผิดปกติ (เช่น บัญชีพนักงานที่ไม่เคยเข้าใช้งานระบบเลย)
- ควรประสานงานกับฝ่ายทรัพยากรบุคคลในการให้ข้อมูลที่ลาออกไปแล้วอย่างทันท่วงที หรือให้ฝ่ายทรัพยากรบุคคลมีหน้าที่ในการลบบัญชีของพนักงานที่ลาออก รวมถึงให้รับผิดชอบต่อการลบหรือเรียกคืนทรัพย์สินทางอิเล็กทรอนิกส์อื่น ๆ เฉกเช่นเดียวกับทรัพย์สินอื่น ๆ ที่พนักงานเคยถือครอง

5) การลบบริการ และแอปพลิเคชันที่ไม่จำเป็นแล้ว เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

- ตรวจสอบบริการ และแอปพลิเคชันต่าง ๆ อย่างสม่ำเสมอ หากไม่มีการใช้งานแล้วควรลบการให้บริการดังกล่าว รวมถึงตรวจสอบว่าถูกควบคุม และเข้าถึงโดยผู้ไม่ได้รับอนุญาต หรือไม่
- ใช้เครื่องมือในการตรวจสอบอัตโนมัติ

6) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

- ตรวจสอบ และสแกนพอร์ต เพื่อตรวจสอบพอร์ตที่ไม่ได้ใช้งาน หรือพอร์ตที่เปิดใช้งานโดยไม่จำเป็น
- ตั้งค่า Firewall Rule เพื่อควบคุมการใช้พอร์ตเท่าที่จำเป็น
- ตรวจสอบข้อมูล Log ของการจราจรเครือข่ายอย่างสม่ำเสมอ และมีขั้นตอนการตอบสนองต่อเหตุการณ์ผิดปกติอย่างทันท่วงที

7) การป้องกันมัลแวร์ (Malware)

- ติดตั้ง และอัพเดตโปรแกรมตรวจจับไวรัส และมัลแวร์อย่างสม่ำเสมอ
- สร้างความตระหนักแก่ผู้ใช้งาน โดยเฉพาะการสร้างอุปนิสัยที่ดีในการเข้าถึงระบบสารสนเทศ หรือเว็บไซต์ที่ปลอดภัย และการดาวน์โหลดไฟล์จากแหล่งที่เชื่อถือได้
- มีระบบเฝ้าระวัง และตอบสนองต่อความผิดปกติของเครือข่ายที่มีสาเหตุมาจากมัลแวร์

8) การปรับปรุงซอฟต์แวร์ และ Patch ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

- มีขั้นตอนในการบริหารจัดการ Patch ซึ่งประกอบไปด้วยการทดสอบ Patch และการอัพเดต Patch

- ต้องทดสอบ Patch และประเมินผลการทดสอบทุกครั้ง ก่อนที่จะอัพเดตในระบบที่ใช้งานจริง

3. ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อ หรือเมื่อมีการเปลี่ยนแปลง หรือปรับปรุงบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- จัดอบรมหรือสัมมนาเพื่อให้พนักงานทุกคนเข้าใจความสำคัญ และสร้างความตระหนักของการรักษาความปลอดภัยไซเบอร์ รวมถึงชี้แจงเกี่ยวกับมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัยที่หน่วยงานต้องใช้ เพื่อให้พนักงานสามารถปฏิบัติตามได้อย่างถูกต้อง
- จัดทำเอกสารแนวทางปฏิบัติที่ชัดเจน โดยอธิบายข้อกำหนดเกี่ยวกับการตั้งค่าระบบ การติดตั้งซอฟต์แวร์ และการใช้งานระบบต่าง ๆ ในรูปแบบที่เข้าใจง่าย รวมถึงบทลงโทษสำหรับผู้ที่ฝ่าฝืน

4. ต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างน้อยปีละ 1 (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

- กำหนดระยะเวลาขั้นต่ำในการตรวจสอบคือ 1 ปี
- มีการตรวจสอบทุกครั้งเมื่อมีการเปลี่ยนแปลงระบบ หรือบริการที่สำคัญ รวมถึงการเปลี่ยนแปลงโครงสร้างหน่วยงาน หรือบุคลากรที่ส่งผลต่อการเปลี่ยนแปลงสิทธิการเข้าถึงระบบ หรือข้อมูล

5. ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ ของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- มีการบันทึกเอกสารเกี่ยวกับการเปลี่ยนแปลงดังกล่าวทุกครั้ง
- มีการจัดตั้งคณะทำงานในการพิจารณาอนุมัติการเปลี่ยนแปลงอย่างเป็นทางการ โดยคณะทำงานควรประกอบไปด้วยผู้มีส่วนได้เสีย ทีมความมั่นคงปลอดภัย และผู้ดูแลระบบ
- ต้องได้รับการอนุมัติอย่างเป็นทางการทุกครั้งก่อนที่จะเริ่มดำเนินการเปลี่ยนแปลงใด ๆ
- ต้องทำการทดสอบฟังก์ชันการทำงาน และความมั่นคงปลอดภัยทุกครั้งก่อนที่จะเปลี่ยนแปลงในระบบจริง
- ต้องสำรวจความพึงพอใจของผู้ใช้งาน และผลกระทบหลังดำเนินการเปลี่ยนแปลงไปแล้ว

แนวทางการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) อ้างอิงจาก ร่างแนวทางการตรวจประเมินตาม (ร่าง) หลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์ และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต โดยศูนย์กำกับดูแลและตรวจสอบธุรกิจ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (10 เมษายน 2566)

1. การกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ โดยครอบคลุมองค์ประกอบของระบบอย่างน้อย ดังนี้

1) ระบบปฏิบัติการบนเครื่องแม่ข่ายและเครื่องลูกข่าย เช่น Window, Unix

2) โปรแกรมมิดเดิลแวร์(middleware) สำหรับเครื่องแม่ข่าย เช่น WebSphere, JBoss, WebLogic, Tomcat, IIS, Nginx

3) โปรแกรมฐานข้อมูลบนเครื่องแม่ข่าย เช่น MS SQL, MySQL, Oracle DB

4) อุปกรณ์เครือข่าย เช่น firewall, switch, router

5) Hypervisor (e.g. VMware ESXi), Containers (e.g. Docker, Kubernetes), Cloud components (e.g. Amazon, Azure, Google, Office365)

2. ตรวจสอบว่ามาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย
คำนึงถึงหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังนี้

1) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

2) การแบ่งแยกหน้าที่ (Separation of Duties)

3) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

4) การลบบัญชีที่ไม่ได้ใช้

5) การลบบริการ และแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application) รวมถึงการให้บริการเข้าถึงผ่านเว็บที่ไม่จำเป็น

6) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

7) การป้องกันมัลแวร์ (Malware)

8) การปรับปรุงซอฟต์แวร์ และ Patch อย่างทันการณ์ และเหมาะสม

9) มีการสอบทานการตั้งค่าอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

3. กรณีมีความจำเป็นต้องตั้งค่าที่ไม่เป็นไปตามเอกสาร Minimum Baseline Standard ควรผ่านกระบวนการขออนุมัติยกเว้น (Exception) เพื่อประเมินความเสี่ยง และพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการ

ตารางที่ 7 แบบประเมินตนเองด้านการทำให้ระบบมีความแข็งแกร่ง (System Hardening)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้นซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. หน่วยงานมีการกำหนดการตั้งค่าระบบ หรืออุปกรณ์โดยอ้างอิงตามมาตรฐานอุตสาหกรรม หรือข้อกำหนดที่ได้รับการยอมรับ หรือไม่		
2. หน่วยงานมีการจัดทำเอกสารมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) หรือไม่		
3. หน่วยงานมีการเปลี่ยนค่ารหัสผ่าน หรือการตั้งค่าจากค่าที่ถูกตั้งไว้ตั้งแต่แรกจากเจ้าของผลิตภัณฑ์ (Default Password / Default Setting) ทุกครั้งก่อนนำไปใช้งานจริง หรือไม่		
4. หน่วยงานมีการใช้เครื่องมืออัตโนมัติในการสแกนช่องโหว่ของระบบอย่างเป็นประจำ หรือไม่		
5. หน่วยงานมีการบริหารจัดการ Patch ที่เหมาะสม ซึ่งประกอบไปด้วยการทดสอบ Patch และอัพเดต Patch อย่างสม่ำเสมอ หรือไม่		
6. หน่วยงานมีขั้นตอนการตรวจสอบบัญชีที่ไม่ได้ใช้งาน และสิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege) หรือไม่		
7. หน่วยงานมีการตรวจสอบข้อมูล Log ของการจราจรเครือข่าย และวิเคราะห์เพื่อค้นหาการเข้าถึงโดยไม่ได้รับอนุญาต และสิ่งผิดปกติอื่น ๆ หรือไม่		
8. หน่วยงานมีการตรวจสอบสิทธิการเข้าถึงโดยอิงตามหน้าที่ความรับผิดชอบอย่างสม่ำเสมอ หรือไม่		
9. หน่วยงานมีการตรวจสอบพอร์ตที่ไม่ได้ใช้งาน และพอร์ตที่เปิดให้บริการโดยไม่จำเป็น และมีการปิดพอร์ตดังกล่าวอย่างสม่ำเสมอ หรือไม่		
10. หน่วยงานมีการติดตั้ง และอัพเดตโปรแกรมตรวจจับไวรัส และมัลแวร์อย่างสม่ำเสมอ หรือไม่		
11. หน่วยงานมีการตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) อย่างน้อยปีละ 1 ครั้ง หรือไม่		
12. หน่วยงานมีกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) ของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ หรือไม่		

5.3. การเชื่อมต่อระยะไกล (Remote Connection)

ขั้นตอนปฏิบัติ

1. ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญ หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกัน และตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

- พิจารณาใช้วิธีการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) สำหรับการเชื่อมต่อระยะไกลทุกกรณี
- พิจารณาใช้ Virtual Private Network (VPN) สำหรับการเชื่อมต่อระยะไกลซึ่งมีการเข้ารหัสระหว่างการรับส่งข้อมูล
- ทำการแยกส่วนเครือข่าย (Network Segmentation) สำหรับการเข้าถึงจากระยะไกลเพื่อเข้าถึงข้อมูลภายในหน่วยงาน
- ทำการตั้ง Firewall Rule เพื่อควบคุมการรับส่งข้อมูลระหว่างผู้ใช้งานจากระยะไกลและระบบที่มีความสำคัญยิ่งยวด
- มีการตรวจสอบ และวิเคราะห์ข้อมูล Log ของการเชื่อมต่อระยะไกลอย่างสม่ำเสมอ
- มีมาตรการรักษาความปลอดภัยที่อุปกรณ์ปลายทาง (Endpoint Security) เช่นติดตั้งโปรแกรม Antivirus หรือระบบตรวจจับ และตอบสนองที่อุปกรณ์ปลายทางแบบรวมศูนย์ (Endpoint Detection and Response (EDR)) เป็นต้น
- จัดฝึกอบรม และสร้างความตระหนักในส่วนของผู้ใช้งานระยะไกล รวมถึงภัยคุกคามที่มักพบบ่อยสำหรับการเชื่อมต่อระยะไกล

2. สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

(ก) *ในกรณีที่เป็นไปได้ให้เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไซต์ระยะไกล เมื่อจำเป็นเท่านั้น*

- อนุญาตการเชื่อมต่อระยะไกลเท่าที่จำเป็นโดยอิงตามนโยบาย บทบาท หน้าที่ ความรับผิดชอบเท่านั้น
- อนุญาตการเชื่อมต่อระยะไกลโดยพิจารณาจากเงื่อนไขอื่น ๆ ที่จำเป็น เช่น ระบุผู้ใช้งานเฉพาะ สถานะความปลอดภัยของอุปกรณ์ สถานที่ (ในประเทศ หรือต่างประเทศ) เป็นต้น

(ข) *ในกรณีที่เป็นไปได้ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง*

- ทำการเข้ารหัสข้อมูลที่จะมีการรับส่งระหว่างการเชื่อมต่อระยะไกล (Transport Layer Security :TLS)
- พิจารณาใช้ลายเซ็นดิจิทัล (Digital Signature) เพื่อใช้ยืนยันที่มา และความถูกต้องของข้อมูล
- พิจารณาใช้โครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure : PKI) เพื่อใช้ยืนยันที่มา และใช้ในการรักษาความลับของข้อมูล

(ค) *ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น*

- พิจารณาการเข้ารหัสในการรับส่งข้อมูลสำหรับการเชื่อมต่อระยะไกลที่เหมาะสมขึ้นอยู่กับวัตถุประสงค์ของการใช้งาน เช่น สำหรับการใช้งานเว็บ การรับส่งไฟล์ การเชื่อมต่อกับเซิร์ฟเวอร์จากระยะไกล เป็นต้น

(ง) *ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการทางธุรกิจ*

- มีวิธีการควบคุมการเข้าถึงอย่างระมัดระวัง เช่น Role-Based Access Control (RBAC) โดยกำหนดเฉพาะกลุ่มผู้ที่มีสิทธิในการใช้คำสั่งระบบจากการเชื่อมต่อระยะไกลเท่านั้น
- กำหนด Whitelist เฉพาะคำสั่งที่สามารถใช้งานได้จากการเชื่อมต่อระยะไกลเท่านั้น
- ตรวจสอบข้อมูล Log ถึงการใช้คำสั่งระบบอย่างสม่ำเสมอ

(จ) *จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ*

- ทำการแยกส่วนเครือข่าย (Network Segmentation) สำหรับการเชื่อมต่อระยะไกลโดยเฉพาะ
- ทำการตั้งค่า Firewall Rule เพื่อควบคุมการไหลของข้อมูลระหว่างเครือข่าย
- ควบคุมการไหลข้อมูลในระดับ Application Layer เช่น ควบคุมการเข้าถึงบางเว็บไซต์ หรือบางระบบสารสนเทศ เป็นต้น
- จำกัดแบนด์วิดท์ (Bandwidth) หรือปริมาณรับส่งข้อมูล
- จัดลำดับความสำคัญของการรับส่งข้อมูล (Quality of Service : QoS) ตามความสำคัญของระบบสารสนเทศ หรือบริการ

ตารางที่ 8 แบบประเมินตนเองด้านการเชื่อมต่อระยะไกล (Remote Connection)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้น ซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. หน่วยงานมีมาตรการควบคุมการเชื่อมต่อระยะไกล หรือไม่		
2. หน่วยงานมีมาตรการควบคุมการเชื่อมต่อระยะไกลในส่วนของเครือข่าย เช่น การแยกส่วนเครือข่าย (Network Segmentation) หรือไม่		
3. หน่วยงานมีมาตรการควบคุมการเชื่อมต่อระยะไกลในส่วนของ Application Layer เช่น การจำกัดการเข้าถึงบางเว็บไซต์ หรือบางระบบ หรือไม่		
4. หน่วยงานมีควบคุมแบนด์วิดท์ (Bandwidth) และจัดลำดับความสำคัญของการรับส่งข้อมูล (Quality of Service : QoS) เมื่อมีการเชื่อมต่อระยะไกล หรือไม่		
5. หน่วยงานมีวิธีการพิสูจน์ตัวตนโดยเฉพาะสำหรับการเชื่อมต่อระยะไกล หรือไม่		
6. หน่วยงานมีการตรวจสอบข้อมูล Log จากการเชื่อมต่อระยะไกล รวมถึงการตรวจสอบการใช้ชุดคำสั่ง (System Command) และการไหลของข้อมูล (Data Flow) เพื่อตรวจสอบความผิดปกติอย่างทันท่วงที หรือไม่		

5.4. สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

ขั้นตอนปฏิบัติ

1. ต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยใช้มาตรการอย่างน้อย ดังนี้

(ก) *ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น*

- พิจารณาออกนโยบายไม่ให้ใช้พอร์ตการเชื่อมต่อภายนอกทั้งหมดเป็นค่าเริ่มต้น (Disable by Default) สำหรับอุปกรณ์ที่ให้บริการที่สำคัญ และบล็อก (Block) การเข้าถึงจากสื่อเก็บข้อมูลแบบถอดได้
- มีระบบการควบคุมการใช้พอร์ตการเชื่อมต่อภายนอก โดยอนุญาตเฉพาะผู้ที่มีสิทธิเท่านั้นตามหน้าที่ความรับผิดชอบ

(ข) *ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตตามหัวข้อ การควบคุมการเข้าถึง (Access Control)*

- มีระบบการลงทะเบียน และอนุมัติสื่อบันทึกข้อมูลที่สามารถใช้งานได้
- มีขั้นตอนการตรวจสอบรายชื่อสื่อบันทึกข้อมูลที่ได้ลงทะเบียนไว้อย่างสม่ำเสมอ

(ค) *ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ*

- ตรวจสอบระดับความมั่นคงปลอดภัยของสื่อบันทึกข้อมูลที่ได้ลงทะเบียนไว้อย่างสม่ำเสมอ โดยอนุญาตให้เฉพาะสื่อที่ผ่านเกณฑ์ระดับความมั่นคงปลอดภัยขั้นต่ำ จึงจะสามารถใช้งานได้

2. ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศบนสื่อบันทึกข้อมูลแบบถอดได้

- แยกแยะประเภทข้อมูลที่มีความละเอียดอ่อน หรือมีชั้นความลับ เพื่อที่จะได้ทำการเข้ารหัส
- เลือกใช้วิธีการเข้ารหัสที่แข็งแรง เพื่อรักษาความลับของข้อมูล (Confidentiality) ในกรณีที่สื่อบันทึกข้อมูลสูญหาย หรือถูกขโมย โดยใช้อัลกอริทึมที่เป็นที่ปลอดภัยและเป็นที่ยอมรับ เช่น AES ที่มีความยาวกุญแจตั้งแต่ 128 บิต ขึ้นไป เป็นต้น
- พิจารณาการเข้ารหัสทั้งไดรฟ์ หรือทั้งสื่อบันทึกข้อมูล หากจำเป็น

ตารางที่ 9 แบบประเมินตนเองด้านการใช้งานสื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้น ซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. หน่วยงานมีมาตรการควบคุมการใช้งานสื่อบันทึกข้อมูลแบบถอดได้ หรือไม่		
2. หน่วยงานมีขั้นตอนในการลงทะเบียน และอนุมัติการใช้งานสื่อบันทึกข้อมูลแบบถอดได้ หรือไม่		
3. หน่วยงานมีการตรวจสอบสื่อบันทึกข้อมูลแบบถอดได้ที่ได้ลงทะเบียนไว้อย่างสม่ำเสมอ หรือไม่		
4. หน่วยงานมีมาตรการที่อนุญาตเฉพาะสื่อบันทึกข้อมูลแบบถอดได้ที่ผ่านเกณฑ์ระดับความมั่นคงปลอดภัยขั้นต่ำ หรือไม่		
5. หน่วยงานมีมาตรการการเข้ารหัสข้อมูลที่อ่อนไหว หรือมีชั้นความลับสูงในสื่อบันทึกข้อมูลแบบถอดได้ หรือไม่		

5.5. การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

ขั้นตอนปฏิบัติ

1. ต้องให้ความสำคัญกับแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมาและผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) *กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่*

- *พนักงานใหม่ (New Employees)*
- *ผู้ใช้ และระดับบริหาร (Users and Management)*
- *เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศเช่น ผู้ให้บริการ IT และ ICS และ*
- *ผู้ขาย ผู้รับเหมา และผู้ให้บริการ (Vendors, Contractors and Service Providers)*

โดยมีรายละเอียดดังนี้

- พัฒนาหลักสูตรอบรมที่แตกต่างกันสำหรับบุคลากรแต่ละประเภท เพื่อให้เนื้อหามีความเหมาะสมกับหน้าที่ ความรับผิดชอบเฉพาะในบุคลากรประเภทนั้น
- ประสานงานกับฝ่ายทรัพยากรบุคคล เพื่อช่วยวิเคราะห์ความจำเป็นด้านความมั่นคงปลอดภัยในบทบาท หน้าที่ความรับผิดชอบของบุคลากรในแต่ละประเภท
- ผนวกหลักสูตรอบรมเข้าไปในกระบวนการของการพัฒนาบุคลากรประจำปีของฝ่ายทรัพยากรบุคคล รวมถึง การสร้างข้อบังคับให้พนักงานใหม่ต้องเข้ารับการอบรมหลักสูตรดังกล่าว
- มีการประเมินผลการอบรมที่เหมาะสม รวมถึงการทำแบบฝึกจำลองในสภาพที่เสมือนจริง (Simulation/Drill) เพื่อทดสอบความตระหนักพนักงานอย่างแท้จริง และฝึกการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น

(ข) *การเผยแพร่ความรับผิดชอบของกลุ่ม และบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ*

- ควรจัดทำเอกสารที่กำหนดบทบาท หน้าที่ความรับผิดชอบสำหรับกลุ่ม และบุคคลเป็นลายลักษณ์อักษรอย่างชัดเจน รวมถึงขั้นตอนในการตอบสนองต่อเหตุการณ์ที่เป็นภัยไซเบอร์ และช่องทางในการติดต่อ และเอกสารดังกล่าวต้องเข้าใจง่ายโดยทุกกลุ่ม
- เผยแพร่เนื้อหาดังกล่าวผ่านการฝึกอบรมเฉพาะกลุ่มในหัวข้อที่แล้วข้างต้น
- มีการสื่อสารแบบ Top-Down ตั้งแต่ระดับบริหารลงมาในการสร้างวัฒนธรรมการรักษาความมั่นคงปลอดภัยแก่บุคลากรทุกคน และสร้างความเข้าใจว่าการรักษาความมั่นคงปลอดภัยเป็นหน้าที่ของทุกคน

(ค) *การตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ*

- สร้างความตระหนักรู้ในกฎระเบียบที่เกี่ยวข้อง ตั้งแต่ ระเบียบ และนโยบายภายในหน่วยงาน ไปจนถึงกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย การคุ้มครองข้อมูลส่วนบุคคล และธุรกรรมอิเล็กทรอนิกส์ เป็นต้น
- ทบทวนระเบียบ และนโนบายภายในอย่างเป็นประจำ และสื่อสารการเปลี่ยนแปลงระเบียบ และนโยบายแก่บุคลากรทุกคนอย่างมีประสิทธิภาพ

(ง) *การสื่อสารอย่างสม่ำเสมอ และทันท่วงทีครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบ*

- ผนวกเรื่องกรณีศึกษา และผลกระทบที่ใกล้ตัว และเข้าใจง่ายในหลักสูตรการฝึกอบรมข้างต้น
- สร้างความเข้าใจ และความสำคัญในการลดผลกระทบ และการตอบสนองต่อภัยคุกคามได้อย่างทันท่วงที (Cyber Resilience) นอกเหนือจากการป้องกันเพียงอย่างเดียว

2. ต้องทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละหนึ่ง (1) ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบัน และมีรายละเอียดที่เกี่ยวข้องเหมาะสม

- ทบทวนแผนงานตามระยะที่กำหนดไว้ และวิเคราะห์ผลการตอบรับจากบุคลากร
- สำรวจความคิดเห็นจากบุคลากรถึงความมีประสิทธิภาพของระเบียบ และนโยบาย รวมถึงปัญหา และอุปสรรคจากการรักษาความมั่นคงปลอดภัยในช่วงที่ผ่านมา
- จัดทำการควบคุมเวอร์ชัน (Version Control) ของระเบียบและนโยบายที่มีการเปลี่ยนแปลง

ตัวอย่างแหล่งเรียนรู้หลักสูตรการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

- TDGA https://tdga.dga.or.th/index.php?option=com_eventbooking&view=event&id=157&catid=35&Itemid=379&lang=th
- NCSA e-Learning https://national-cyber-academy.ncsa.or.th/open-elearning/
- AIS อุ่นใจไซเบอร์ https://learndiaunjaicyber.ais.co.th/
- Cyber Safe Kids https://www.cybersafekids.cyberlitebooks.com/
- IT Chula https://www.youtube.com/watch?v=DWVN_nYYM38
- กรมควบคุมโรค https://www.facebook.com/dddc.ddc/videos/465821538444677

ตารางที่ 10 แบบประเมินตนเองด้านการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้นซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. หน่วยงานมีการจัดฝึกอบรมความตระหนักในการรักษาความมั่นคงปลอดภัยเป็นประจำ หรือไม่		
2. หน่วยงานมีการพัฒนาหลักสูตรอบรมที่แตกต่างกันสำหรับบุคลากรแต่ละประเภท หรือไม่		
3. หน่วยงานมีสื่อสารแบบ Top-Down ในเรื่องการรักษาความมั่นคงปลอดภัย หรือไม่		
4. หน่วยงานมีการจัดทำเอกสารที่แสดงหน้าที่ ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสำหรับบุคลากรแต่ละประเภท หรือไม่		
5. หน่วยงานมีการทบทวนแผนการฝึกอบรมเป็นประจำ หรือไม่		

5.6. การแบ่งปันข้อมูล (Information Sharing)

ขั้นตอนปฏิบัติ

1. ต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูล เกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์ หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบ หรืออาจเกิดขึ้นได้ ได้รับผลกระทบจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ หรือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ (เช่น ผู้ใช้ ผู้รับเหมาที่ให้บริการแก่บริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และเจ้าของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ) เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้

- กำหนดช่องทาง และผู้ที่เกี่ยวข้องในการแบ่งปันข้อมูลให้ชัดเจน และจะต้องสื่อสารให้กับบุคลากร และผู้มีส่วนได้เสียทุกคนได้ทราบ
- กำหนดเกณฑ์ของการเป็นเหตุการณ์ หรือภัยคุกคามทางไซเบอร์ที่จะต้องรายงานแก่ผู้ที่เกี่ยวข้อง รวมถึงการต้องแจ้งตามที่กำหนดไว้ในกฎหมาย เช่น การแจ้งหน่วยงานกำกับหรือผู้ที่ได้รับผลกระทบ
- แยกประเภทหมวดหมู่ชั้นความลับ และความอ่อนไหวของข้อมูล และมีขั้นตอนในการแบ่งปันข้อมูลแต่ละประเภทที่แตกต่างกัน
- มีช่องทางในการแบ่งปันข้อมูลแบบปลอดภัย และมีการเข้ารหัสข้อมูลหากข้อมูลนั้นเป็นความลับ หรือมีความอ่อนไหว
- ก่อนทำการแบ่งปันข้อมูล ควรพิจารณาเรื่องการคุ้มครองข้อมูลส่วนบุคคลด้วย และหากมีข้อมูลส่วนบุคคลที่ไม่จำเป็นต้องแบ่งปัน จะต้องทำให้ข้อมูลนั้นเป็นข้อมูลนิรนามเสียก่อน (Anonymization)
- มีข้อตกลงในการแบ่งปันข้อมูลกับหน่วยงานภายนอก โดยคำนึงถึงความมั่นคงปลอดภัย ธรรมาภิบาลข้อมูล และไม่ขัดต่อกฎหมายที่เกี่ยวข้อง และระดับความมั่นคงปลอดภัยและธรรมาภิบาลข้อมูลของหน่วยงานภายนอกควรจะอยู่ระดับเดียวกันหรือสูงกว่าหน่วยงานเจ้าของข้อมูล
- สร้างวัฒนธรรมการแบ่งปันข้อมูลข้ามฝ่ายงานภายในหน่วยงาน และระหว่างหน่วยงาน
- มีระบบแจ้งเตือน และตอบสนองต่อภัยคุกคามแบบ Real Time และอัตโนมัติ
- ทบทวนประสิทธิภาพ และผลกระทบของการแบ่งปันข้อมูลอย่างเป็นประจำ

รายละเอียด แนวทาง และรูปแบบในการแบ่งปันข้อมูล เพื่อความเป็นมาตรฐานในการปฏิบัติงานและสามารถใช้ข้อมูลได้อย่างมีประสิทธิภาพ ให้เป็นไปตามหลักเกณฑ์ และวิธีการที่สำนักงานประกาศกำหนด

ทั้งนี้ แนวทางในการแบ่งปันข้อมูลหรือแลกเปลี่ยนข้อมูล จะต้องคำนึงถึงการรักษาธรรมาภิบาลข้อมูลเป็นหลัก ซึ่งสามารถศึกษาได้จากเอกสารธรรมาภิบาลข้อมูลภาครัฐ โดยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

https://standard.dga.or.th/standards-manual/dgf-ebook/2576/ และศึกษาแนวทางการจัดทำข้อมูลนิรนาม (Anonymization) จัดทำโดย Personal Data Protection Commission Singapore และร่วมแปลโดยสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล https://www.nstda.or.th/nstdaxpdpc/privacytools/

ตารางที่ 11 แบบประเมินตนเองด้านการแบ่งปันข้อมูล (Information Sharing)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้นซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. หน่วยงานมีการกำหนดเกณฑ์ หรือคำจำกัดความที่ชัดเจนของการเป็นเหตุการณ์หรือภัยคุกคามไซเบอร์ หรือไม่		
2. หน่วยงานมีการกำหนดช่องทางที่ชัดเจนในการแบ่งปันข้อมูล หรือไม่		
3. หน่วยงานมีการแบ่งแยกขั้นตอนในการแบ่งปันข้อมูลตามประเภทชั้นความลับของข้อมูล หรือไม่		
4. หน่วยงานมีการดำเนินการเฉพาะเพื่อคุ้มครองข้อมูลส่วนบุคคลก่อนการแบ่งปันข้อมูล เช่น การจัดทำข้อมูลนิรนาม (Anonymization) หรือไม่		
5. หน่วยงานมีการจัดทำข้อตกลงในการแบ่งปันข้อมูลกับหน่วยงานภายนอก หรือไม่		

6. มาตรการตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

มาตรการตรวจสอบ และเฝ้าระวัง (Detect) เป็นด่านป้องกันชั้นแรกจากเหตุการณ์ด้านไซเบอร์ การตรวจจับความผิดปกติของระบบ พฤติกรรมผู้ใช้งาน หรือการโจมตีที่อาจเกิดขึ้น จะส่งผลให้สามารถรับมือกับภัยคุกคามได้ทันท่วงที ป้องกันความเสียหายที่ร้ายแรง ลดอัตราความสำเร็จของการโจมตี และทำให้การกู้คืนระบบรวดเร็วขึ้น มาตรการตรวจสอบ และเฝ้าระวังเปรียบเสมือนเป็นระบบเตือนภัยที่ช่วยให้รับรู้ถึงความเสี่ยง หรือภัยอันตรายก่อนที่จะสายเกินแก้ ดังนั้น การมีมาตรการตรวจสอบ และเฝ้าระวังที่มีประสิทธิภาพจึงเป็นพื้นฐานสำคัญในการบริหารความเสี่ยงด้านไซเบอร์อย่างมีประสิทธิผล

การตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

ขั้นตอนปฏิบัติ

1. ต้องสร้างกลไก และกระบวนการเพื่อ

(ก) *ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ*

- ใช้เครื่องมือในการตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ที่เหมาะสมกับหน่วยงาน
- ใช้เครื่องมือในการตรวจสอบข้อมูล Log และกิจกรรมเครือข่าย (Network Activity) อย่างสม่ำเสมอ และมีการตอบสนองต่อเหตุการณ์ที่ผิดปกติ เช่น Security Information and Event Management (SIEM) ซึ่งเป็นเครื่องมือรวบรวมและวิเคราะห์ข้อมูล Log เพื่อหาสิ่งผิดปกติ, Security Orchestration, Automation, and Response (SOAR) ที่ช่วยดำเนินการตอบสนองต่อเหตุการณ์อัตโนมัติ และ Threat Intelligence ซึ่งเป็นระบบที่รวบรวมและวิเคราะห์ข้อมูลด้านภัยคุกคามทางไซเบอร์ เป็นต้น
- มีระบบแจ้งเตือนแบบเรียลไทม์ (Real Time) สำหรับเหตุการณ์ที่ผิดปกติ หรือน่าสงสัย
- พิจารณาจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operations Center: SOC) หรือใช้บริการ SOC จากผู้ให้บริการภายนอก สำหรับหน่วยงานที่ขาดบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์หรือต้องการเฝ้าระวังตลอด 24 ชั่วโมง หน่วยงานสามารถพิจารณาใช้ Opensource SOC หากต้องการลดค่าใช้จ่ายค่าซอฟต์แวร์แต่ต้องใช้ทรัพยากรบุคคลและเวลาในการเรียนรู้

(ข) *การจัดประเภท และวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ*

- มีการวิเคราะห์ข้อมูลการแจ้งเตือน และ Log เพื่อระบุว่าเป็นภัยคุกคามแบบใด
- มีการเชื่อมโยงเหตุการณ์ต่าง ๆ เหล่านี้ เพื่อระบุขอบเขต และความร้ายแรงของภัยคุกคาม
- จัดประเภทเหตุการณ์ที่ผิดปกติที่วิเคราะห์ได้จากพฤติกรรมของผู้ใช้งานในหน่วยงาน (Behavior Analytics)

(ค) *การระบุว่ามีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือไม่*

- วิเคราะห์ความเสี่ยง และผลกระทบที่เกิดขึ้นจากภัยคุกคาม หรือเหตุการณ์ดังกล่าวว่าส่งผลต่อบริการ หรือหน่วยงานมากน้อยเพียงใด
- เตรียมความพร้อมในการตอบสนองต่อภัยคุกคาม หรือเหตุการณ์ดังกล่าว ซึ่งประกอบไปด้วย
  - มีขั้นตอนการปฏิบัติงานของทีมตอบสนอง (Incident Response Team) และกำหนดบทบาท และความรับผิดชอบชัดเจน
  - มีการแยก (Isolation) ระบบ หรือเครือข่ายที่ได้รับผลกระทบออกจากระบบอื่น ๆ เพื่อจำกัดความเสียหาย
  - มีการรวบรวมข้อมูลหลักฐานจากเหตุการณ์ดังกล่าว เพื่อใช้ในการวิเคราะห์ต่อไป
  - มีการควบคุมยับยั้งเหตุ และป้องกันโดยทันที เพื่อไม่ให้ภัยคุกคามนั้นกระจายในวงกว้าง
  - มีการจัดการกับซอฟต์แวร์ประสงค์ร้าย (Malicious Software) หรือการเข้าถึงที่ไม่ได้รับอนุญาตจากระบบที่ได้รับผลกระทบ
  - มีการปิดช่องโหว่ (Patching) และเพิ่มความแข็งแกร่งของระบบ (Hardening)
  - มีการวิเคราะห์ถึงต้นตอของเหตุการณ์ และผลกระทบ
  - มีการบันทึกบทเรียนที่ได้ และข้อเสนอแนะสำหรับการปรับปรุงกระบวนการทำงานในอนาคต
  - มีการทบทวน หรือแก้ไขนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยจากการวิเคราะห์เหตุการณ์ที่เกิดขึ้น
  - มีการแจ้งเหตุไปยังผู้ที่เกี่ยวข้อง และผู้มีส่วนได้เสียอย่างเหมาะสม
  - มีการรายงานเหตุไปยังหน่วยงานกำกับ และผู้ที่เกี่ยวข้องตามที่กฎหมาย หรือระเบียบต่าง ๆ ที่ได้ระบุไว้
  - มีการสื่อสารไปยังผู้ที่ได้รับผลกระทบถึงสิ่งที่ต้องปฏิบัติอย่างเป็นขั้นตอน เพื่อลดผลกระทบ

2. ต้องดำเนินการทบทวนกลไก และกระบวนการภายในข้อ 1. อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ากลไก และกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

ตารางที่ 12 แบบประเมินตนเองด้านการตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้นซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. การกำหนดขอบเขตของภัยคุกคาม		
• จากเหตุภัยคุกคามทั้งหมดที่เคยส่งผลกระทบต่อหน่วยงาน หน่วยงานได้มีการบันทึกเหตุการณ์ และผลการวิเคราะห์เป็นเอกสารในทุกเหตุการณ์ หรือไม่		
• หน่วยงานได้มีความเข้าใจอย่างถ่องแท้ถึงผลกระทบของภัยคุกคามในแต่ประเภท หรือไม่		
• หน่วยงานมีข้อกำหนด หรือบรรทัดฐานที่สามารถนำมาใช้ เพื่อระบุได้ว่าเหตุการณ์ที่เกิดขึ้นจะถือว่าเป็นเหตุภัยคุกคามด้านความมั่นคงปลอดภัย หรือไม่		
2. การบันทึก Log และการตรวจสอบ		
• มีระบบบันทึก Log ส่วนกลาง (Centralized Logging System) ในระบบที่มีความสำคัญสูง และระบบเครือข่าย หรือไม่		
• มีการตรวจสอบข้อมูล Log ทั้งหมด เพื่อค้นหาเหตุการณ์ที่น่าสงสัย หรือเหตุภัยคุกคาม หรือไม่		
• มีระบบแจ้งเตือนแบบเรียลไทม์เมื่อเกิดเหตุภัยคุกคาม หรือไม่		
3. ระบบตรวจสอบ และป้องกันการบุกรุก (Intrusion Detection and Prevention Systems (IDPS))		
• มีการอัพเดตระบบตรวจสอบ และป้องกันการบุกรุกอย่างสม่ำเสมอ เพื่อป้องกันภัยคุกคามแบบใหม่		
• มีขั้นตอนการตรวจสอบว่าระบบตรวจสอบ และป้องกันการบุกรุกยังมีการทำงานที่ถูกต้อง และมีประสิทธิภาพ • เมื่อระบบตรวจสอบ และป้องกันการบุกรุกมีการแจ้งเตือนเหตุแล้ว หน่วยงานมีระบบ หรือเครื่องมือสำหรับการตรวจสอบ หรือตอบสนองต่อการแจ้งเตือนนั้น หรือไม่		

คำถาม	ใช่	ไม่ใช่
4. การตรวจสอบช่องโหว่ (Vulnerability Assessment) และการทดสอบการเจาะระบบ (Penetration Testing)		
• มีการตรวจสอบช่องโหว่ และการทดสอบการเจาะระบบอย่างเป็นประจำ หรือไม่		
• มีตารางกำหนดการทดสอบดังกล่าว และผู้ที่ทำการทดสอบมีคุณสมบัติที่เหมาะสม หรือไม่		
• มีการนำผลการทดสอบไปวิเคราะห์ และแก้ไขหลังจากนั้น หรือไม่		
5. แผนการตอบสนอง (Incident Response Plan)		
• มีการจัดทำเอกสารแผนการตอบสนองที่กำหนดบทบาท และความรับผิดชอบภายในทีม หรือไม่		
• บุคลากรในทีมตอบสนองได้รับทราบถึงบทบาทของตนเอง และได้รับการฝึกอบรมในบทบาทเฉพาะของตนเอง หรือไม่		
• แผนการตอบสนองได้มีการทดสอบผ่านเหตุการณ์จำลอง (Simulation) หรือไม่		
6. การตรวจสอบ และวิเคราะห์อย่างต่อเนื่อง		
• มีการตรวจสอบข้อมูล Log และรายงานเพื่อวิเคราะห์เหตุที่น่าสงสัย หรือการเข้าถึงที่ไม่ได้รับอนุญาตอย่างเป็นประจำ หรือไม่		
• มีขั้นตอนในการเชื่อมโยงเหตุการณ์เพื่อวิเคราะห์ไปถึงภัยคุกคาม หรือไม่		
• มีเครื่องมือ หรือทรัพยากรที่เหมาะสม และเพียงพอในการตรวจสอบ และวิเคราะห์ข้อมูล Log และรายงาน หรือไม่		
7. นโยบาย และขั้นตอน		
• มีการทบทวน และอัพเดตนโยบาย และขั้นตอนอย่างเป็นประจำ โดยอ้างอิงจากเหตุการณ์ที่เคยเกิดขึ้น หรือกรณีศึกษาจากหน่วยงานอื่น ๆ หรือไม่		
• มีวิธี หรือขั้นตอนในการสื่อสารถึงการอัพเดตนโยบาย และขั้นตอนดังกล่าว ไปยังบุคลากรที่เกี่ยวข้องทุกคน หรือไม่		
• พนักงานทุกคนได้รับการฝึกอบรมในเรื่องนโยบาย และขั้นตอนดังกล่าว หรือไม่ (หมายถึง เฉพาะเรื่องนโยบาย และขั้นตอนของหน่วยงาน ไม่ใช่เรื่องความรู้ความมั่นคงปลอดภัยในหัวข้ออื่น)		
8. การจัดทำรายงาน และเอกสาร		

คำถาม	ใช่	ไม่ใช่
• มีการกำหนดมาตรฐานการจัดทำรายงาน และเอกสารรายงานเหตุการณ์ หรือไม่		
• มีการรายงานเหตุภัยคุกคามไปยังผู้มีส่วนได้เสียทุกคน รวมถึงผู้บริหาร และฝ่ายกฎหมายอย่างครบถ้วน และอย่างรวดเร็ว หรือไม่		
• เอกสารรายงานดังกล่าวมีความครบถ้วนสมบูรณ์ ประกอบไปด้วยรายละเอียดเหตุภัยคุกคาม ผลกระทบ และขั้นตอนการแก้ไขอย่างละเอียด หรือไม่		

7. มาตรการรับมือภัยคุกคามทางไซเบอร์ (Respond)

การรับมือภัยคุกคามทางไซเบอร์ (Respond) มีความสำคัญยิ่ง เพราะเป็นหัวใจสำคัญของ Cyber Resilience หรือความสามารถในการรับมือ ปรับตัว และฟื้นฟูจากเหตุการณ์ด้านไซเบอร์ ซึ่งเป็นแนวคิดใหม่ที่มองว่า มาตรการป้องกันไม่เพียงต่อการปกป้องข้อมูล เนื่องจากแม้ว่าจะมีการป้องกันที่ดีเพียงใด ย่อมมีโอกาสที่จะถูกโจมตีได้เสมอ มาตรการรับมือภัยคุกคามทางไซเบอร์ จึงมุ่งเน้นการตอบสนองที่รวดเร็ว และเหมาะสมเมื่อเกิดเหตุการณ์ ด้วยการประเมินสถานการณ์ จำกัดความเสียหาย กำหนดแผนดำเนินการ สื่อสารภายในและภายนอก ช่วยให้ควบคุมสถานการณ์ ลดผลกระทบ และกู้คืนระบบได้อย่างรวดเร็ว การฝึกซ้อมแผนรับมือ (Cybersecurity Incident Response Plan) บุคลากรที่มีความพร้อม และการเรียนรู้จากเหตุการณ์ที่เกิดขึ้นล้วนเป็นองค์ประกอบสำคัญของการรับมือ ซึ่งเสริมสร้างความยืดหยุ่น และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในอนาคต

7.1. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

ขั้นตอนปฏิบัติ

ต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพ และประสิทธิผล

7.1.1 จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

7.1.1.1โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาท และความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคน และรายละเอียดการติดต่อ

- การกำหนดบทบาทชัดเจนในแต่ละคน เช่น ผู้ประสานงาน ผู้รับผิดชอบด้านเทคนิค ผู้รับผิดชอบด้านกฎหมาย ผู้รับผิดชอบด้านการสื่อสารภายใน และภายนอก เป็นต้น
- การแจ้งช่องทางการติดต่อของผู้ประสานงานหลัก ผู้ประสานงานรอง และผู้เกี่ยวข้องอื่น ๆ ช่องทางติดต่อ ได้แก่ เบอร์โทรศัพท์ อีเมล แอปฯ หรือ ช่องทางใด ๆ
- การกำหนดข้อมูลที่จำเป็นที่จะต้องแจ้ง หรือรายงานไปยังทีม CIRT
- การกำหนดเกณฑ์ และเงื่อนไขว่าเหตุการณ์ใดถึงจะต้องแจ้งทีม CIRT หรือจะเริ่มนำแผนมาปฏิบัติ

- การวางแผนการฝึกอบรม และการฝึกซ้อมรับมือ (Drill) ของทีม CIRT เพื่อสำรวจความพร้อมในการทำงานของทีม และต้องกำหนดเป็นแผนประจำ

หน่วยงานขนาดเล็กที่มีทรัพยากรจำกัดก็ยังคงสามารถนำแนวคิดการทำงานของทีม CIRT ไปปรับใช้ได้ดังนี้

- หน่วยงานขนาดเล็กอาจไม่จำเป็นต้องมีทีม CIRT ขนาดใหญ่ แต่สามารถแต่งตั้งบุคลากรภายในทำหน้าที่ในการดูแลการรับมือเหตุการณ์ได้และควรได้รับการฝึกอบรมเพิ่มเติมอย่างสม่ำเสมอ
- ใช้เครื่องมือด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่มีค่าใช้จ่ายหรือเป็นโอเพนซอร์ส (Open Source) สำหรับระบบตรวจสอบและบันทึกกิจกรรม (SIEM) เครื่องมือสแกนช่องโหว่ (Vulnerability Scanner) และเครื่องมือสำหรับการวิเคราะห์พยานหลักฐานดิจิทัล (Forensics) เช่น Wazuh, GRR Rapid Response, TheHive, Volatility เป็นต้น
- อาศัยความร่วมมือกับหน่วยงานภายนอก ซึ่งหน่วยงานควรจะหาโอกาสในการเข้าร่วมกลุ่ม สมาคมหรือกิจกรรมด้านความมั่นคงปลอดภัยไซเบอร์หรือด้านที่เกี่ยวข้อง เพื่อสร้างความร่วมมือแลกเปลี่ยนประสบการณ์และความช่วยเหลือซึ่งกันและกัน

7.1.1.2โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- ศึกษากฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 เป็นต้น ว่ามีข้อบังคับในการรายงานหน่วยงานที่เกี่ยวข้อง หรือไม่อย่างไร
- กำหนดช่วงระยะเวลาในการรายงานหน่วยงานให้ชัดเจน เพื่อไม่ให้เกินระยะเวลาที่กำหนด
- จัดทำเอกสารรายงานเพื่อใช้เป็นหลักฐานในภายหลัง เช่น เพื่อการตรวจสอบหรือการสืบสวน

7.1.1.3เกณฑ์ และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

- กำหนดเกณฑ์ที่ชัดเจนในการเริ่มแผนปฏิบัติการ เช่น ระดับของความเสียหาย ความผิดปกติของระบบ หรือรูปแบบการถูกโจมตี เป็นต้น และเกณฑ์ หรือขั้นตอนจะต้องชัดเจน และเข้าใจได้ง่ายโดยบุคลากรที่เกี่ยวข้องของหน่วยงาน
- กำหนดขั้นตอนในการปฏิบัติงานในช่วงเวลาที่ไม่ปกติ เช่น เวลาหลังเลิกงาน วันหยุดยาว หรือเมื่อเกิดเหตุด่วนที่ส่งผลกระทบในวงกว้าง เป็นต้น

- กำหนดวิธีในการระดมทีม CIRT และผู้ที่เกี่ยวข้องในรูปแบบต่าง ๆ เมื่อเกิดเหตุ เช่น การประชุมกันในห้องประชุม หรือรูปแบบออนไลน์

7.1.1.4ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

- แยก หรือตัดระบบที่ได้รับผลกระทบออกมาจากเครือข่ายโดยทันทีเพื่อป้องกันเหตุที่จะขยายผลไปยังส่วนอื่น ๆ
- ควบคุมการเข้าถึงระบบที่ได้รับผลกระทบโดยเข้มงวดในช่วงที่เกิดเหตุ โดยอนุญาตเฉพาะผู้ที่เกี่ยวข้องเท่านั้น
- ดำเนินการวิเคราะห์ และแก้ไขปัญหาที่ต้นเหตุของเหตุการณ์ผิดปกตินั้น
- ทบทวน และอัพเดตส่วนที่เกี่ยวข้อง เช่น Firewall Rule, Intrusion Prevention System, Patch, การควบคุมการเข้าถึง เป็นต้น
- อัพเดต Endpoint Security เช่น Antivirus, Antimalware และสแกนระบบที่ได้รับผลกระทบเพื่อมั่นใจได้ว่าซอฟต์แวร์ หรือไฟล์ที่ผิดปกติได้ถูกกำจัดไปแล้ว

7.1.1.5การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

- จัดทำแผนการกู้คืน โดยมีการจัดลำดับความสำคัญของระบบ และข้อมูลที่จะกู้คืน
- ในการกู้คืน ต้องมั่นใจว่าไม่มีสิ่งผิดปกติ เช่น Malware หรือช่องโหว่ใด ๆ หลงเหลืออยู่
- สื่อสารกับผู้มีส่วนได้เสียถึงกระบวนการกู้คืน และผลกระทบในระหว่างนั้น
- จัดทำเอกสารเพื่อบันทึกทุกขั้นตอนในการกู้คืนนั้น เช่น การเปลี่ยนแปลงการตั้งค่าใด ๆ เพื่อเก็บไว้เป็นหลักฐาน และเพื่อการปรับปรุงการทำงานในอนาคต

7.1.1.6ขั้นตอนในการสอบสวน (Investigate) สาเหตุ และผลกระทบของเหตุการณ์

- รวบรวมหลักฐาน เช่น ไฟล์ Log, ข้อมูลการจราจรเครือข่าย และข้อมูลหลักฐานอื่น ๆ ประกอบกับข้อมูลช่วงเวลา เพื่อสืบหาต้นตอของเหตุ
- จัดลำดับความสำคัญในการสอบสวนตามระบบที่ได้รับผลกระทบมากที่สุด
- ร่วมมือประสานงานกับหน่วยงานภายนอกที่เกี่ยวข้อง เช่น หน่วยงานกำกับหน่วยงานที่ดูแลกฎหมายที่เกี่ยวข้อง หน่วยงานด้านการสืบสวน หน่วยงานผู้มีส่วนได้เสีย เป็นต้น
- วิเคราะห์ต้นตอของเหตุเพื่อที่จะได้แก้ไข และป้องกันได้ถูกจุด
- ตรวจสอบว่าจากเหตุที่เกิดขึ้น จะต้องดำเนินการตามกฎหมายหรือไม่ เช่น รายงานไปยังหน่วยงานกำกับ หรือหน่วยงานที่ดูแลกฎหมายที่เกี่ยวข้อง การบันทึกข้อมูลเพื่อเก็บไว้เป็นหลักฐานในการสอบสวน เป็นต้น

7.1.1.7ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

- บันทึกการดำเนินงาน (Chain of Custody) อย่างละเอียด ตั้งแต่การเก็บหลักฐาน การควบคุมการเข้าถึง การส่งต่อ หรือรับมอบ จนถึงการทำลายพยานหลักฐาน ข้อมูลเหล่านี้รวมถึงข้อมูลบุคคลที่จัดการกับหลักฐาน เวลาในการรวบรวมหลักฐาน และการเปลี่ยนแปลงต่าง ๆ ในช่วงเวลาการสอบสวน
- มีขั้นตอนการดูแลหลักฐานที่เชื่อมั่นว่าหลักฐานไม่ถูกแก้ไข หรือเปลี่ยนแปลง เช่น การป้องกันการเขียนทับ (Write-Protected) การแฮชไฟล์ (Hash) เป็นต้น
- มีการควบคุมการเข้าถึงหลักฐาน และจัดเก็บหลักฐานด้วยวิธีแบบปลอดภัย

7.1.1.8ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืน และการบังคับใช้กฎหมายเพื่อดำเนินคดี

- มีการลงนามในข้อตกลงรักษาความลับ (Non-Disclosure Agreement)
- มีช่องทางในการติดต่อสื่อสาร หรือแลกเปลี่ยนข้อมูลกับบุคคลภายนอกด้วยวิธีแบบปลอดภัย
- กำหนดขอบเขตการมีส่วนร่วม และความรับผิดชอบของบุคคลภายนอกอย่างชัดเจน เช่น บทบาท หน้าที่ ระยะเวลา รวมถึงการควบคุมการเข้าถึงเครือข่าย ข้อมูล และระบบสารสนเทศ

7.1.1.9กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุ และแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

- รวบรวมความคิดเห็นจากผู้ที่เกี่ยวข้องทั้งหมด เช่น ทีม CIRT ทีม IT ผู้บริหาร และผู้มีส่วนได้เสียหลักอื่น ๆ
- ประเมินประสิทธิภาพในการดำเนินงาน และวิเคราะห์ปัจจัยสำคัญ เช่น ระยะเวลาในการดำเนินการ ผลลัพธ์ในการดำเนินการทางเทคนิค ผลลัพธ์ของการสื่อสารทั้งภายในและภายนอก เป็นต้น
- วิเคราะห์จุดแข็ง และจุดอ่อนของการดำเนินการ
- ตรวจสอบให้แน่ชัดว่าแผนดังกล่าวเป็นไปตามวัตถุประสงค์ หรือเป้าหมายของหน่วยงาน หรือไม่ และแผนดังกล่าวได้คำนึงถึงผลประกอบการของหน่วยงานด้วย หรือไม่
- ถอดบทเรียน บันทึกลงเอกสาร และปรับปรุงแผนปฏิบัติการที่มีอยู่จากการถอดบทเรียน

- ปรับปรุง หรืออัพเดตนโยบาย แนวปฏิบัติ และหลักสูตรการสร้างความตระหนักแก่พนักงาน จากการถอดบทเรียนตามความเหมาะสม

7.1.2 การสื่อสารแผนการรับมือภัยคุกคาม (Communication of Cybersecurity Incident Response Plan)

ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

แนวทางการสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์มีดังนี้

- วางแผนการสื่อสารแผนการรับมือภัยคุกคามด้วยวิธีที่เหมาะสมกับหน่วยงาน รวมถึงช่องทางการสื่อสาร ข้อความที่จะสื่อสาร และผู้รับผิดชอบในการสื่อสารไปยังบุคคลต่าง ๆ ในหน่วยงาน
- มีการตรวจสอบว่าพนักงานทุกคนที่เกี่ยวข้องได้รับการสื่อสารแผนการรับมือภัยคุกคามและสามารถเข้าใจได้

7.1.3 การทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ (Review Cybersecurity Incident Response Plan)

ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ

ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ตัวอย่างของการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น

- การเปลี่ยนแปลง หรืออัพเกรดระบบสารสนเทศในหน่วยงานอย่างมีนัยสำคัญ เช่น การเปลี่ยน Vendor ฮาร์ดแวร์ หรือซอฟต์แวร์ การเปลี่ยนเวอร์ชันของระบบที่มีการเปลี่ยนแปลงไปอย่างมาก เป็นต้น
- การเปลี่ยนโครงสร้างองค์กร หรือการโยกย้าย หรือเปลี่ยนตำแหน่งที่สำคัญของบุคลากร
- การเปลี่ยนแปลงกฎหมาย ระเบียบ นโยบาย หรือแนวปฏิบัติ

ตัวอย่างการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์

- มาตรฐานและแนวปฏิบัติของ สกมช. https://ncsa.or.th/standards-and-practices.html
- ร่าง ประกาศ สพร. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) https://standard.dga.or.th/

- กรอบการประเมินความพร้อมด้าน Cyber Resilience โดย ธนาคารแห่งประเทศไทย

https://www.bot.or.th/content/dam/bot/fipcs/documents/FOG/2562/ThaiPDF/25620189.pdf

ตารางที่ 13 แบบประเมินตนเองด้านแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้น ซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. หน่วยงานมีแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) หรือไม่		
2. หน่วยงานมีการกำหนดบทบาทชัดเจนในแต่ละคนในการรับมือภัยคุกคาม หรือไม่		
3. หน่วยงานมีการกำหนดเกณฑ์ และเงื่อนไขว่าเหตุการณ์ใดถึงจะต้องแจ้งทีม CIRT หรือจะเริ่มนำแผนมาปฏิบัติ หรือไม่		
4. หน่วยงานมีการวางแผนการฝึกอบรม และการฝึกซ้อมรับมือ (Drill) ของทีม CIRT หรือไม่		
5. หน่วยงานมีการกำหนดขั้นตอนชัดเจนในการรายงานเหตุภายใต้กฎหมายที่เกี่ยวข้อง หรือไม่		
6. หน่วยงานมีการจัดทำเอกสารรายงาน เพื่อเก็บไว้เป็นหลักฐานในภายหลัง หรือไม่		
7. หน่วยงานมีขั้นตอนการจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ หรือไม่		
8. หน่วยงานมีการจัดทำแผนการกู้คืน (Recovery Process) หรือไม่		
9. หน่วยงานมีกระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) หรือไม่		
10. หน่วยงานมีแนวปฏิบัติการบริหารจัดการบุคคลภายนอกในส่วนที่เกี่ยวข้องกับการตอบสนองต่อภัยคุกคาม หรือไม่ เช่น การลงนามในข้อตกลงรักษาความลับ การมีช่องทางสื่อสารกับบุคคลภายนอกแบบปลอดภัย การควบคุมการเข้าถึงโดยบุคคลภายนอก เป็นต้น		
11. หน่วยงานมีกระบวนการสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ไปยังบุคลากรที่เกี่ยวข้องทุกคนอย่างมีประสิทธิภาพ หรือไม่		

คำถาม	ใช่	ไม่ใช่
12. หน่วยงานมีการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ 1 ครั้ง หรือไม่		

7.2. แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

ขั้นตอนปฏิบัติ

1. ต้องจัดทำแผนการสื่อสารในภาวะวิกฤต เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

- กำหนดขั้นตอน และช่องทางที่ชัดเจนในการสื่อสารในภาวะวิกฤต เพื่อให้มั่นใจว่าข้อมูลจะถูกสื่อสารออกไปได้อย่างรวดเร็ว และสามารถเชื่อถือได้

2. ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต

(ก) *จัดตั้งทีมสื่อสารในภาวะวิกฤต เพื่อเปิดใช้งานในช่วงวิกฤต*

- มอบหมายบุคลากร หรือทีมที่ทำหน้าที่สื่อสารในภาวะวิกฤตให้ชัดเจน เพื่อให้ข้อมูลที่จะถูกสื่อสารมาจากแหล่งเดียว และไม่ขัดแย้งกันเอง
- ควรคำนึงถึงการสื่อสารที่รวดเร็ว เนื่องจากผู้มีส่วนได้เสียซึ่งเป็นผู้ได้รับผลกระทบจำเป็นจะต้องทราบข้อมูลสำหรับการรับมือ
- ควรคำนึงถึงความถูกต้องของข้อมูล มีการตรวจสอบความถูกต้อง และความทันสมัยของข้อมูลที่สุดก่อนสื่อสารออกไป
- ควรคำนึงถึงความโปร่งใสของข้อมูล รวมถึงการยอมรับผลกระทบที่เกิดขึ้นเพื่อสร้างความไว้วางใจแก่ผู้มีส่วนได้เสียในการติดตามสถานการณ์
- ควรคำนึงถึงการรักษาความลับ โดยเฉพาะข้อมูลที่อ่อนไหว หรือข้อมูลส่วนบุคคลที่ไม่จำเป็นต้องเปิดเผย แต่ต้องพิจารณาร่วมกับการสร้างความโปร่งใสของข้อมูล
- ควรคำนึงถึงความเข้าอกเข้าใจของผู้ได้รับผลกระทบ และคำนึงถึงเนื้อหาที่จะต้องสื่อสารออกไปในการแสดงความรู้สึกเข้าอกเข้าใจ รวมถึงแนวทางในการดำเนินการต่อไป เพื่อลดผลกระทบหรือชดเชย

(ข) *ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง*

(ค) *ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้เสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท*

- นอกจากนี้ ควรระบุหน่วยงานที่เกี่ยวข้องที่จะต้องรายงานตามกฎหมายด้วย โดยเฉพาะหน่วยงานกำกับ และต้องศึกษาข้อกำหนดในการรายงานตามภาระหน้าที่ทางกฎหมายด้วย เช่น รายงานเมื่อได้รับผลกระทบ หรือความเสี่ยงในระดับใด รายงานภายในระยะเวลาเท่าใดหลังเกิดเหตุ เป็นต้น

(ง) *ระบุโฆษกหลัก และผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กร เมื่อกล่าวแถลงกับสื่อมวลชน*

- ควรเลือกผู้เชี่ยวชาญด้านเทคนิคที่มีความรู้อย่างถ่องแท้ต่อเหตุการณ์ที่เกิดขึ้น

- ควรสื่อสารในรูปแบบที่เข้าใจง่าย หลีกเลี่ยงศัพท์เทคนิคเฉพาะจนเกินไป

(จ) *ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล*

- นอกจากนี้ ควรจัดเตรียมรูปแบบ หรือ Template ในการสื่อสารในภาวะวิกฤตในสถานการณ์ต่าง ๆ ซึ่งต้องประกอบด้วยข้อมูลที่จำเป็น เช่น รายละเอียดเหตุการณ์ แนวทางการรับมือ และแนวทางปฏิบัติสำหรับผู้ที่ได้รับผลกระทบ เป็นต้น

3. ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบ เพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกัน และสอดคล้องกันในช่วงวิกฤต

4. ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ 1 (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสาร และเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ตัวอย่างการสื่อสารในภาวะวิกฤต

ตัวอย่างที่ 1: เว็บไซต์ล่ม

สถานการณ์: เว็บไซต์ของหน่วยงานล่ม ไม่สามารถให้บริการประชาชนได้ ส่งผลกระทบต่อการเข้าถึงข้อมูลหรือบริการ

การสื่อสาร:

- สื่อสารอย่างรวดเร็วและชัดเจน: หน่วยงานต้องทราบทันทีว่าจะต้องทำอย่างไร โดยผู้ใด ภายในระยะเวลาเท่าใด ซึ่งบุคคลที่รับผิดชอบควรแจ้งสถานการณ์ที่เกิดขึ้นกับประชาชนผ่านช่องทางต่าง ๆ เช่น เว็บไซต์สำรอง โซเชียลมีเดีย โดยระบุสาเหตุของปัญหา แนวทางแก้ไข และระยะเวลาที่คาดว่าจะกลับมาให้บริการได้ตามปกติ
- สร้างความเชื่อมั่น: การสื่อสารอย่างจริงใจ โปร่งใส และอัพเดตข้อมูลอย่างต่อเนื่อง ช่วยสร้างความเชื่อมั่นให้กับประชาชน

ตัวอย่างที่ 2: ข่าวลือโจมตีระบบ

สถานการณ์: มีข่าวลือแพร่สะพัดในโซเชียลมีเดียว่า ข้อมูลของหน่วยงานถูกแฮกเกอร์โจมตี ทำให้ข้อมูลประชาชนรั่วไหลและสร้างความวิตกกังวลให้กับประชาชน

การสื่อสาร:

- สื่อสารอย่างรวดเร็วและชัดเจน: หน่วยงานต้องทราบทันทีว่าจะต้องทำอย่างไร โดยผู้ใด ภายในระยะเวลาเท่าใด และที่สำคัญคือต้องพิสูจน์ว่าข่าวลือนั้นเป็นจริงหรือไม่ ซึ่งบุคคลที่รับผิดชอบในฐานะตัวแทนหน่วยงานควรออกมาชี้แจงข้อเท็จจริงเกี่ยวกับข่าวลืออย่างรวดเร็ว ผ่านช่องทางสื่อสารอย่างเป็นทางการ และควรประสานงานกับหน่วยงานกำกับหรือหน่วยงานที่ต้องแจ้งเหตุข้อมูลรั่วตามกฎหมายเพื่อขอคำแนะนำ และหาแนวทางในการแก้ไขร่วมกัน
- รักษาภาพลักษณ์หน่วยงาน: ควรคำนึงถึงการตอบสนองต่อข่าวลืออย่างรวดเร็วและจริงใจ เพื่อช่วยป้องกันความเสียหายต่อชื่อเสียงของหน่วยงาน

ตารางที่ 14 แบบประเมินตนเองแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้น ซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. หน่วยงานมีการกำหนดขั้นตอน และช่องทางที่ชัดเจนในการสื่อสารในภาวะวิกฤต หรือไม่		
2. หน่วยงานมีการจัดตั้งทีมสื่อสารในภาวะวิกฤต เพื่อเปิดใช้งานในช่วงวิกฤต หรือไม่		
3. หน่วยงานมีการระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียในแต่ละสถานการณ์ รวมถึงการระบุหน่วยงานที่เกี่ยวข้องที่จะต้องรายงานตามกฎหมายด้วย หรือไม่		
4. หน่วยงานมีการระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม หรือไม่		
5. หน่วยงานมีการจัดเตรียมรูปแบบ หรือ Template ในการสื่อสารในภาวะวิกฤตในสถานการณ์ต่าง ๆ ซึ่งต้องประกอบด้วยข้อมูลที่จำเป็น หรือไม่		
6. หน่วยงานมีการดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ 1 ครั้ง หรือไม่		

7.3. การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

ขั้นตอนปฏิบัติ

1. ตามมาตรา 22 วรรคหนึ่ง (13) ของ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 กำหนดให้หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำโดยคณะกรรมการ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าว อาจดำเนินการได้ ทั้งในระดับชาติ หรือระดับภาคส่วน หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

- กำหนดวัตถุประสงค์ของการฝึกซ้อมให้ชัดเจน
- รวบรวมผู้มีส่วนได้เสียให้ครบถ้วน ซึ่งต้องมาจากหลายฝ่าย เช่น เทคโนโลยีสารสนเทศความมั่นคงปลอดภัยไซเบอร์ กฎหมาย และฝ่ายที่เกี่ยวข้องกับพันธกิจหลักของหน่วยงาน นอกจากนี้ยังเป็นการฝึกซ้อมการประสานงานข้ามฝ่ายอีกด้วย
- ออกแบบสถานการณ์จำลองเสมือนจริงที่จะส่งผลกระทบต่อหน่วยงาน เช่น สถานการณ์ข้อมูลรั่วไหล ระบบถูกโจมตีด้วยมัลแวร์ เป็นต้น
- ทำการฝึกซ้อมโดยยึดแนวทางตามแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) และถือเป็นการทดสอบแผนดังกล่าวด้วย
- เชิญหน่วยงานภายนอก เช่น หน่วยงานภาครัฐโดยเฉพาะหน่วยงานกำกับภาคอุตสาหกรรม หรือผู้มีส่วนได้เสียหลักจากภายนอกเข้าร่วมสังเกตการณ์ และร่วมแลกเปลี่ยนความคิดเห็น
- ทำการซ้อมแผนบนโต๊ะ (Table Top Exercise) หรือการฝึกซ้อมแบบไม่เป็นทางการบนพื้นฐานสถานการณ์สมมติ ก่อนที่จะทดสอบเต็มรูปแบบที่จำลองสถานการณ์เสมือนจริง เพื่อทดสอบแผนการรับมือเบื้องต้นว่าสามารถใช้ได้จริง หรือไม่
- ประเมินเทคโนโลยีที่มีอยู่ว่ามีความพร้อมในการรับมือต่อเหตุภัยคุกคาม และสามารถกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ หรือไม่
- จัดทำเอกสารวิเคราะห์บทเรียนที่ได้จากการฝึกซ้อม อันจะส่งผลต่อการแก้ไขนโยบาย ขั้นตอน และเทคโนโลยีที่มีอยู่ในปัจจุบัน
- ประสานงานกับหน่วยงานกำกับ เพื่อยืนยันว่าการฝึกซ้อมนี้เป็นไปตามข้อกำหนดทางกฎหมาย หรือข้อแนะนำในระดับอุตสาหกรรม
- วิเคราะห์ผลตอบรับจากผู้เข้าร่วมฝึกซ้อม เพื่อใช้เป็นแนวทางในการออกแบบการฝึกซ้อมในครั้งถัดไปในอนาคต

2. ต้องปฏิบัติตามคำขอใด ๆ ของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์ และแผนการสื่อสารในภาวะวิกฤตที่กำหนดขึ้นตามขั้นตอนการปฏิบัติงานตามมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญ ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- ประสานงานกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์เมื่อถูกร้องขอข้อมูล นอกจากนี้ควรประสานกับหน่วยงานกำกับ หรือคณะกรรมการอื่น ๆ ที่กำกับดูแลด้วยเช่น สำนักงานรัฐบาลดิจิทัล (องค์การมหาชน) (สำหรับหน่วยงานภาครัฐ) สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หน่วยงานกำกับด้านหลักทรัพย์และตลาดหลักทรัพย์ ด้านการเงิน การธนาคาร เป็นต้น
- จัดทำบันทึกเป็นเอกสาร เพื่อเก็บเป็นหลักฐานในการส่งข้อมูลเมื่อถูกร้องขอ

ตารางที่ 15 แบบประเมินตนเองการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้นซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. หน่วยงานมีการวางแผนการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์เป็นลายลักษณ์อักษร หรือไม่		
2. หน่วยงานมีการกำหนดวัตถุประสงค์ของการฝึกซ้อมให้ชัดเจน หรือไม่		
3. หน่วยงานมีการรวบรวมผู้มีส่วนได้เสียให้ครบถ้วนซึ่งมาจากหลายฝ่าย หรือไม่		
4. หน่วยงานทำการฝึกซ้อมโดยยึดแนวทางตามแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) หรือไม่		
5. หน่วยงานได้มีการเชิญหน่วยงานภายนอกเข้ามาร่วมสังเกตุการณ์ และแลกเปลี่ยนความคิดเห็น หรือไม่		
6. หน่วยงานมีการประสานงานกับหน่วยงานกำกับในการฝึกซ้อม หรือไม่		
7. หน่วยงานมีการจัดทำเอกสารวิเคราะห์บทเรียนที่ได้จากการฝึกซ้อม หรือไม่		
8. หน่วยงานมีการบันทึกหลักฐานการส่งข้อมูลเมื่อถูกร้องขอไปยังคณะกรรมการ หรือหน่วยงานกำกับที่เกี่ยวข้อง หรือไม่		

8. มาตรการรักษา และฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

มาตรการรักษา และฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามมุ่งเน้นการฟื้นฟูระบบสารสนเทศ ข้อมูล และการดำเนินงานของหน่วยงาน หลังประสบเหตุการณ์โจมตี มาตรการรักษา และฟื้นฟูความเสียหายนี้จะช่วยให้ระบบสารสนเทศ ข้อมูล และการดำเนินงานของหน่วยงานที่ได้รับผลกระทบ กลับมาดำเนินงานได้อย่างต่อเนื่อง และรวดเร็ว ด้วยวิธีการต่าง ๆ เช่นการสำรองข้อมูล การกู้คืนระบบ การสื่อสารเพื่อสร้างความเชื่อมั่นให้กับผู้มีส่วนได้เสีย การบรรเทาผลกระทบทางธุรกิจ การเรียนรู้จากข้อผิดพลาด และปรับปรุงมาตรการป้องกันให้ดีขึ้น ดังนั้นมาตรการนี้จึงไม่ใช่แค่การกู้คืนเพียงอย่างเดียว แต่เป็นการเสริมสร้างความแข็งแกร่งป้องกันไม่ให้เหตุการณ์ซ้ำรอย สร้างความมั่นใจในความปลอดภัยของข้อมูล ระบบสารสนเทศ และหน่วยงานในระยะยาว

การรักษา และฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

ขั้นตอนปฏิบัติ

1. ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอกเพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ความสอดคล้องกันของขอบเขตคำนิยาม และการกำหนดระยะเวลาที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ให้เป็นไป ตามหลักเกณฑ์ และวิธีการที่สำนักงานประกาศกำหนด

- เตรียมข้อมูลในการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ซึ่งอย่างน้อยประกอบไปด้วยบทบาท ความรับผิดชอบ และกลยุทธ์ในการสื่อสาร
- วิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) ซึ่งเป็นการวิเคราะห์หาส่วนงานธุรกิจ หรือกระบวนการที่มีความสำคัญ หรือส่งผลกระทบมากที่สุด ซึ่งการวิเคราะห์ลักษณะนี้จะคล้ายกับการวิเคราะห์ความเสี่ยง แต่ใน BIA จะเน้นไปที่กระบวนการทางธุรกิจที่เกี่ยวข้อง การพึ่งพากันในกระบวนการทางธุรกิจ และการจัดลำดับความสำคัญในการกู้คืนข้อมูล ตัวอย่างเช่น กระบวนการสั่งอาหารต้องมาก่อนกระบวนการส่งอาหาร หรือกระบวนการสั่งจองสินค้าต้องมาก่อนกระบวนการจ่ายเงิน และแต่ละกระบวนการต้องพึ่งพากันและกัน ในส่วนของการจัดลำดับความสำคัญในการกู้คืนข้อมูล จะมีหลายปัจจัยที่ต้องพิจารณา เช่น ผลกระทบทางธุรกิจ ระยะเวลาในการกู้คืน และทรัพยากรที่มี เป็นต้น ตัวอย่างการวิเคราะห์การจัดลำดับการกู้คืน เช่น กระบวนการขายควรได้รับการกู้คืนก่อนกระบวนการจัดส่งสินค้า หรือกระบวนการที่ระบุค่า RTO ที่ต่ำกว่า ต้องได้รับการกู้คืนก่อน (เนื้อหา RTO จะถูกอธิบายในส่วนถัดไป)

- กำหนดระยะเวลาที่ระบบหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption : MTPD) ของแต่ละระบบ ซึ่งหมายถึงหากเกินกำหนดเวลานี้จะไม่สามารถทำให้ธุรกิจกลับคืนสู่สภาพปกติได้ เช่น กำหนดให้ระบบเครือข่ายคอมพิวเตอร์มีระยะเวลานานที่สุดที่ยอมให้หยุดชะงักได้ 3 ชั่วโมง

- กำหนดระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objective : RTO)ซึ่งหมายถึงระยะเวลาเป้าหมายที่ใช้ในการดำเนินการเพื่อให้กระบวนการกลับคืนสู่สภาพปกติหลังเกิดเหตุการณ์ เช่น ผู้รับจ้างต้องรับประกันแต่ละระบบต้องกลับมาใช้งานได้ไม่เกิน (Recovery Time Objective: RTO) 4 ชั่วโมง

- กำหนดจุดเป้าหมายเวลาที่ข้อมูลจะได้รับการกู้กลับคืนมา (Recovery Point Objective : RPO) ซึ่งหมายถึงการกำหนดจุดสุดท้ายในการสำรองข้อมูลที่จะสามารถยอมรับการสูญหายของข้อมูลได้เท่าใด เช่น ผู้รับจ้างต้องรับประกันข้อมูลสูญหายของแต่ละระบบไม่เกิน 24 ชั่วโมง

  - วิเคราะห์ความเสี่ยง และจัดทำกลยุทธ์เพื่อลดความเสี่ยง
  - จัดทำแผนในการทดสอบแผนความต่อเนื่องทางธุรกิจ
  - จัดหาสถานที่สำรองในการทำงาน และการจัดเก็บข้อมูลในกรณีที่เกิดเหตุ และทำให้ธุรกิจหยุดชะงัก ซึ่งสถานที่สำรองจะช่วยให้ธุรกิจสามารถดำเนินงานต่อไปได้ โดยมีผลกระทบน้อยที่สุด
  - เตรียมการสื่อสารในภาวะวิกฤต
  - จัดทำระบบสำรองข้อมูล และระบบ Redundancy เพื่อให้มั่นใจว่าระบบอยู่ในสภาพพร้อมใช้ตลอดเวลา
  - ตรวจสอบการทำงานของระบบควบคุมการเข้าถึง (Access Control) อย่างเข้มงวดทั้งระบบจริง และระบบสำรอง เนื่องจากในช่วงเกิดเหตุ ระบบควบคุมการเข้าถึงอาจไม่ได้ทำงานอย่างมีประสิทธิภาพ

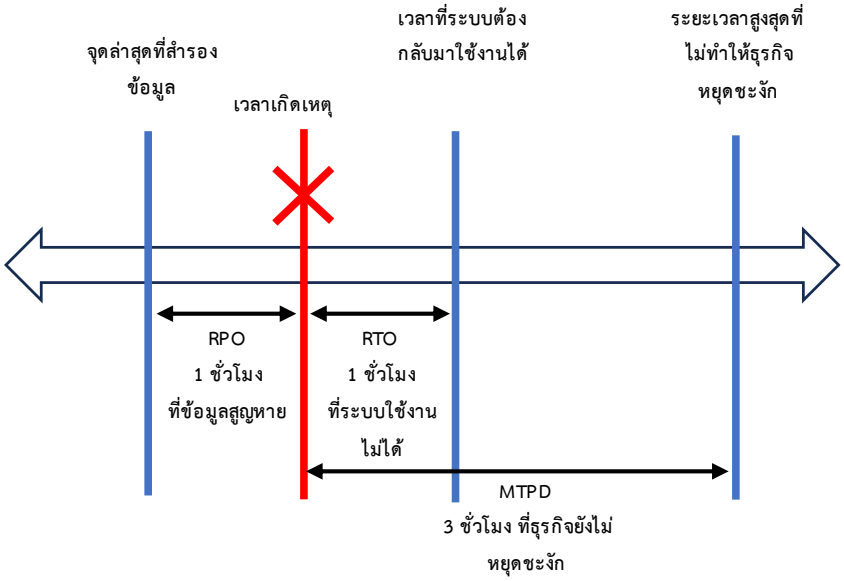
2. ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละ 1 (หนึ่ง) ครั้งเพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์ และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

- จัดฝึกอบรมในเรื่องแผนความต่อเนื่องทางธุรกิจ และควรให้มีการซักซ้อมเสมือนจริง
- จัดทำเอกสาร และบันทึกบทเรียนที่ได้จากการใช้แผนความต่อเนื่องทางธุรกิจในแต่ละครั้ง

ตัวอย่างการกำหนดค่า MTPD RTO และ RPO อยู่ในตัวอย่างด้างล่างนี้

ระบบ	MTPD	RTO	RPO
ระบบเครือข่าย	3 ชั่วโมง	1 ชั่วโมง	1 ชั่วโมง
ระบบสำรองข้อมูล	12 ชั่วโมง	2 ชั่วโมง	10 นาที
ระบบประชุมผ่านสื่ออิเล็กทรอนิกส์	30 นาที	10 นาที	10 นาที
ระบบเว็บไซต์หน่วยงาน	3 ชั่วโมง	1 ชั่วโมง	2 ชั่วโมง

จากตัวอย่างข้างต้น ถ้าเจาะจงไปที่ระบบเครือข่ายที่กำหนด MTPD ไว้ที่ 3 ชั่วโมง RTO 1 ชั่วโมง และ RPO 1 ชั่วโมงแล้ว จะสามารถอธิบายด้วยรูปภาพด้านล่างนี้



รูปที่ 2 แสดงความสัมพันธ์ของเวลา RPO RTO และ MTPD

ตารางด้านล่างนี้ คือตัวอย่างขั้นตอนการวิเคราะห์ผลกระทบทางธุรกิจ (BIA) โดยย่อ

กระบวนการ	คำอธิบาย
1) ระบุกระบวนการ/กิจกรรมหลัก	ผู้อำนวยการกอง ระบุกระบวนการ/กิจกรรมหลักที่เกี่ยวข้องกับการส่งมอบสินค้า/บริการ ที่อยู่ภายใต้ขอบเขตของการพัฒนาระบบบริหารจัดการความต่อเนื่องทางธุรกิจ ซึ่งกระบวนการ/กิจกรรมหลักส่วนใหญ่จะเป็นส่วนที่เกี่ยวข้องกับลูกค้า/ผู้ใช้บริการโดยตรง หากขาดกระบวนการ/กิจกรรมเหล่านี้แล้วจะส่งผลให้องค์กรไม่สามารถบรรลุวัตถุประสงค์ในการส่งมอบสินค้า/บริการได้ ทั้งนี้ แต่ละกระบวนการ/กิจกรรมหลักให้ระบุผู้รับผิดชอบที่เกี่ยวข้อง
2) ระบุทรัพยากรที่จำเป็น	ผู้อำนวยการกอง ระบุทรัพยากรที่จำเป็นต้องใช้ในการดำเนินการตามกระบวนการ/กิจกรรมหลักที่ระบุไว้ โดยพิจารณาทรัพยากรทั้ง 8 ด้าน ดังนี้ 1) บุคลากร

กระบวนการ	คำอธิบาย
	2) สารสนเทศ และข้อมูล 3) อาคาร สภาพแวดล้อมการทำงาน และสาธารณูปโภค 4) สิ่งอำนวยความสะดวก อุปกรณ์ และโภคภัณฑ์ 5) ระบบเทคโนโลยีสารสนเทศและการสื่อสาร 6) การขนส่ง 7) การเงิน 8) ผู้ให้บริการ
3) กำหนดหลักเกณฑ์การวิเคราะห์ผลกระทบทางธุรกิจ	ฝ่ายเลขานุการคณะกรรมการบริหารความต่อเนื่องทางธุรกิจ กำหนดหลักเกณฑ์ที่จะใช้ในการวิเคราะห์ผลกระทบทางธุรกิจ โดยสามารถจำแนกออกเป็นผลกระทบในด้านต่าง ๆ ที่ควรคำนึงถึง และกำหนดวิธีการคำนวณคะแนนของผลกระทบ
4) พิจารณาอนุมัติหลักเกณฑ์การวิเคราะห์ผลกระทบทางธุรกิจ	คณะกรรมการบริหารความต่อเนื่องทางธุรกิจ พิจารณาอนุมัติหลักเกณฑ์การวิเคราะห์ผลกระทบทางธุรกิจ - อนุมัติ: ดำเนินการตามขั้นตอนที่ 5 - ไม่อนุมัติ: ดำเนินการตามขั้นตอนที่ 3
5) วิเคราะห์ผลกระทบทางธุรกิจ	ผู้อำนวยการกอง ร่วมกันวิเคราะห์ผลกระทบทางธุรกิจของกระบวนการ/กิจกรรมหลักตามเกณฑ์การวิเคราะห์ผลกระทบทางธุรกิจที่ระบุไว้
6) ระบุค่า RTO, RPO, MTPD และ MBCO	ผู้อำนวยการกอง ร่วมกันระบุค่า RTO, RPO, MTPD และ MBCO
7) จัดลำดับความสำคัญของกระบวนการ/กิจกรรมหลัก	ผู้อำนวยการกอง ร่วมกันจัดลำดับความสำคัญของกระบวนการ/กิจกรรมหลักและความสัมพันธ์ที่เกี่ยวข้องกันของแต่ละกระบวนการ/กิจกรรมหลัก
8) พิจารณาอนุมัติผลการวิเคราะห์ผลกระทบทางธุรกิจ	ผู้อำนวยการฝ่าย พิจารณาอนุมัติผลการวิเคราะห์ผลกระทบทางธุรกิจ ค่า RTO, RPO, MTPD และ MBCO และผลการจัดลำดับความสำคัญของกระบวนการ/กิจกรรมหลัก - อนุมัติ: เข้าสู่กระบวนการประเมินความเสี่ยง - ไม่อนุมัติ: ดำเนินการตามขั้นตอนที่ 5

ตัวอย่างการกำหนดเกณฑ์การประเมินผลกระทบในการทำ BIA เป็นดังนี้

คะแนน	ผลกระทบ	ด้านการเงิน	ด้านชื่อเสียงและภาพลักษณ์ขององค์กร	ด้านผู้มีส่วนได้ส่วนเสียขององค์กร	ด้านการปฏิบัติตามกฎระเบียบ/ข้อบังคับ
1	ต่ำมาก	ขาดรายได้หรือเกิดค่าใช้จ่ายในการซ่อมแซม/ดำเนินการ คิดเป็นจำนวนเงินน้อยกว่า 500,000 บาท	มีผลกระทบน้อยมากหรือไม่มีเลย	มีผลกระทบต่อคุณภาพการให้บริการและประสิทธิภาพในการปฏิบัติงานน้อยมากหรือไม่มีเลย	มีผลกระทบน้อยมากหรือไม่มีเลย
2	ต่ำ	ขาดรายได้หรือเกิดค่าใช้จ่ายในการซ่อมแซม/ดำเนินการ คิดเป็นจำนวนเงิน 500,000 ถึง 1,000,000 บาท	มีผลกระทบน้อยผู้ใช้บริการเกิดความไม่พอใจแต่อยู่ในระดับที่ยอมรับได้	มีผลกระทบต่อคุณภาพการให้บริการและประสิทธิภาพในการปฏิบัติงานน้อย แต่อยู่ในระดับที่ยอมรับได้	ส่งผลกระทบชั่วคราวเป็นระยะเวลาไม่เกิน 1 วัน ไม่เกิดข้อพิพาทหรือการฟ้องร้อง
3	ปานกลาง	ขาดรายได้หรือเกิดค่าใช้จ่ายในการซ่อมแซม/ดำเนินการ คิดเป็นจำนวนเงิน 1,000,0000 ถึง 3,000,000 บาท	มีผลกระทบต่อชื่อเสียงขององค์กรในมุมมองของสาธารณชนผู้ใช้บริการเกิดความไม่พอใจ	มีผลกระทบต่อคุณภาพการให้บริการและประสิทธิภาพในการปฏิบัติงานปานกลางการให้บริการของ	ส่งผลกระทบชั่วคราวเป็นระยะเวลาไม่เกิน 1 สัปดาห์ ไม่เกิดข้อพิพาทหรือการฟ้องร้อง

คะแนน	ผลกระทบ	ด้านการเงิน	ด้านชื่อเสียงและภาพลักษณ์ขององค์กร	ด้านผู้มีส่วนได้ส่วนเสียขององค์กร	ด้านการปฏิบัติตามกฎระเบียบ/ข้อบังคับ
				พนักงานขาดประสิทธิภาพ	
4	สูง	ขาดรายได้หรือเกิดค่าใช้จ่ายในการซ่อมแซม/ดำเนินการ คิดเป็นจำนวนเงิน 3,000,0000 ถึง 5,000,000 บาท	ปรากฏในข่าวและสื่อต่างๆ ผู้ใช้บริการเกิดความไม่พอใจ มีข้อตำหนิจากผู้ใช้บริการ	มีผลกระทบต่อคุณภาพการให้บริการและประสิทธิภาพในการปฏิบัติงานสูง ส่งผลกระทบต่อความพึงพอใจของผู้ใช้บริการ	เกิดข้อพิพาทหรือการฟ้องร้องส่งผลกระทบมากกว่า 1 สัปดาห์ แต่ไม่เกิน 2 สัปดาห์

สามารถศึกษาตัวอย่างการกำหนดค่า MTPD, RTO และ RPO และการจัดทำ BIA เพิ่มเติมได้ตามเอกสารต่อไปนี้

- ตัวอย่างการกำหนด RTO และ RPO ในข้อกำหนดขอบเขตของงาน (TOR) https://www.dga.or.th/wp-content/uploads/2021/12/TOR-DGA-65-0089.pdf
- ตัวอย่างการกำหนด MTPD RTO และ RPO ในแผนบริหารความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศ กรมวิทยาศาสตร์การแพทย์ กระทรวงสาธารณสุข https://www3.dmsc.moph.go.th/download/BCPIT66.pdf
- ตัวอย่างการจัดทำ BIA ในแผนบริหารความต่อเนื่อง กรมท่าอากาศยาน กระทรวงคมนาคม https://www.airports.go.th/backend/uploads/files/83002ec6d076399e20cf6edc8e55d6b2.pdf

ตารางที่ 16 แบบประเมินตนเองด้านการรักษา และฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้น ซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. หน่วยงานมีการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) หรือไม่		
2. หน่วยงานมีการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA) หรือไม่		
3. หน่วยงานมีการกำหนดระยะเวลาที่ระบบหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption : MTPD) ของแต่ละระบบ หรือไม่		
4. หน่วยงานมีการกำหนดระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objective : RTO) หรือไม่		
5. หน่วยงานมีการกำหนดจุดเป้าหมายเวลาที่ข้อมูลจะได้รับการกู้กลับคืนมา (Recovery Point Objective : RPO) หรือไม่		
6. หน่วยงานมีการจัดหาสถานที่สำรอง หรือไม่		
7. หน่วยงานมีการจัดทำระบบสำรองข้อมูล และระบบ Redundancy หรือไม่		
8. หน่วยงานมีการจัดฝึกอบรมในเรื่องแผนความต่อเนื่องทางธุรกิจ และซักซ้อมเสมือนจริง หรือไม่		
9. หน่วยงานมีการจัดทำเอกสาร และบันทึกบทเรียนที่ได้จากการใช้แผนความต่อเนื่องทางธุรกิจในแต่ละครั้ง หรือไม่		

9. ข้อแนะนำเพิ่มเติมทางเทคนิคสำหรับผู้ดูแลระบบ และนักพัฒนาระบบ

เทคโนโลยีสารสนเทศได้เข้ามาเป็นส่วนสำคัญในชีวิตประจำวันของเรา ขับเคลื่อนการพัฒนาในทุกภาคส่วน ไม่ว่าจะเป็นความมั่นคงของประเทศ ธุรกิจ การศึกษา การสาธารณสุข และการสื่อสาร เป็นต้น เทคโนโลยีสารสนเทศช่วยเพิ่มประสิทธิภาพการทำงาน ทำให้เราสามารถทำงานต่าง ๆ ได้รวดเร็ว แม่นยำ ประหยัดเวลาและค่าใช้จ่าย เช่น การจัดการบัญชี การติดต่อสื่อสารออนไลน์ การเก็บข้อมูลบนคลาวด์ และการค้นหาข้อมูลต่าง ๆ เทคโนโลยีสารสนเทศช่วยเพิ่มโอกาสทางธุรกิจโดยการขยายช่องทางการการค้า เช่น การขายสินค้าออนไลน์ และการใช้โซเชียลมีเดียเพื่อโปรโมทธุรกิจ นอกจากนี้เทคโนโลยีสารสนเทศยังช่วยพัฒนาคุณภาพชีวิตในหลายด้าน เช่น ด้านการศึกษา ช่วยให้ผู้เรียนสามารถเข้าถึงข้อมูลได้สะดวกขึ้น ทุกที่ ทุกเวลา และด้านการแพทย์ ช่วยให้ผู้ที่อยู่ห่างไกลสามารถได้รับคำปรึกษา หรือการรักษาโดยแพทย์ผู้ชำนาญผ่านระบบออนไลน์ได้

ถึงแม้ว่าเทคโนโลยีสารสนเทศจะมีประโยชน์มากมาย แต่ด้วยลักษณะของเทคโนโลยีที่เป็นแบบเปิด ไร้พรมแดน และใคร ๆ ก็สามารถเข้าถึงได้ จึงมีภัยคุกคามทางไซเบอร์ที่ผู้ไม่ประสงค์ดีอาจฉวยโอกาสใช้แสวงหาประโยชน์เข้าสู่ตนเอง และสร้างความเสียหายให้กับบุคคล และหน่วยงานต่าง ๆ ได้ มิจฉาชีพสามารถโจมตีระบบคอมพิวเตอร์ เครือข่าย และข้อมูลเพื่อขโมยข้อมูลสำคัญ เรียกค่าไถ่ หรือสร้างความเสียหายโปรแกรมประสงค์ร้าย หรือมัลแวร์แอบแฝงมากับไฟล์ข้อมูล หรือแอปพลิเคชันที่มาจากแหล่งไม่น่าเชื่อถือสามารถสร้างความเสียหายให้กับระบบ และเปิดช่องให้มิจฉาชีพเข้าสู่ระบบโดยไม่ได้รับอนุญาตได้ การโจมตีเพื่อปฏิเสธการให้บริการ (DoS / DDoS) ทำให้ระบบล่มไม่สามารถให้บริการได้ สามารถสร้างความเสียหายให้กับกิจการได้ เป็นต้น

ภัยคุกคามทางไซเบอร์สร้างความเสียหายร้ายแรงต่อทั้งบุคคล ธุรกิจ และประเทศชาติ การปกป้องความมั่นคงทางไซเบอร์จึงเป็นสิ่งที่จำเป็นอย่างยิ่ง การปกป้องความมั่นคงปลอดภัยไซเบอร์ที่ดีควรจะต้องดำเนินการครอบคลุมในทุกระดับชั้น ไม่ว่าจะเป็นระดับโครงสร้างพื้นฐาน เช่น เซิร์ฟเวอร์ ศูนย์ข้อมูล คลาวด์ และระบบเครือข่าย ระดับแอปพลิเคชัน ไม่ว่าจะเป็นแอปพลิเคชันแบบออฟไลน์ หรือแบบออนไลน์ และระดับข้อมูล ซึ่งเป็นสิ่งที่ขับเคลื่อน และพัฒนาโลกของเราทุกวันนี้ ในบทนี้มีการนำเสนอแนวปฏิบัติที่ดีในการลดความเสี่ยงและความเสียหายจากการถูกโจมตีทางไซเบอร์ และการรับมือเบื้องต้น ตั้งแต่การเตรียมความพร้อม การป้องกัน การตรวจสอบ และการฟื้นฟู ครอบคลุมหัวข้อดังต่อไปนี้

1) **แนวปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยคลาวด์** กล่าวถึงพื้นฐานเกี่ยวกับคลาวด์ ได้แก่ ลักษณะสำคัญ แบบจำลองการบริการ และแบบจำลองการจัดเตรียมระบบ และแนะนำแนวปฏิบัติเบื้องต้นสำหรับผู้ใช้งานคลาวด์ และผู้ดูแลระบบ

2) **แนวปฏิบัติสำหรับการพัฒนา และใช้ API อย่างมั่นคงปลอดภัย** กล่าวถึงพื้นฐานเกี่ยวกับ API โดยเฉพาะประเภทของ API อธิบายความเสี่ยงความมั่นคงปลอดภัยของ API ที่พบได้บ่อย และแนวปฏิบัติที่ดีเบื้องต้นเพื่อการรักษาความมั่นคงปลอดภัย

3) แนวปฏิบัติสำหรับการพัฒนาโค้ดอย่างมั่นคงปลอดภัย กล่าวถึงความหมายของการพัฒนาโค้ดและความจำเป็นของการพัฒนาโค้ดอย่างมั่นคงปลอดภัย อธิบายช่องโหว่ความมั่นคงปลอดภัยที่พบบ่อย และแนะนำแนวทางปฏิบัติที่ดีเบื้องต้นเพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

4) แนวปฏิบัติการจัดการการกำหนดค่า กล่าวถึงความหมายของการจัดการกำหนดค่า ความสำคัญและประโยชน์ของการจัดการการกำหนดค่าโดยเฉพาะในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และนำเสนอแนวปฏิบัติที่ดีเบื้องต้นในการจัดการกำหนดค่า

5) แนวปฏิบัติการป้องกัน และรับมือแรนซัมแวร์ กล่าวถึงลักษณะสำคัญของแรนซัมแวร์ ช่องทางการแพร่กระจายของแรนซัมแวร์ และนำเสนอแนวทางการป้องกัน การรับมือ และการตอบสนองต่อการโจมตีด้วยแรนซัมแวร์เพื่อลดความเสี่ยง และผลกระทบต่อผู้ใช้งานทั่วไป และหน่วยงาน

6) แนวปฏิบัติการเพิ่มความมั่นคงปลอดภัยให้กับแอปพลิเคชัน และระบบปฏิบัติการ กล่าวถึงความสำคัญของการเพิ่มความมั่นคงปลอดภัยให้กับแอปพลิเคชันก่อนจะนำไปใช้ในสภาพแวดล้อมการทำงานจริง และระบบปฏิบัติการ และแนะนำแนวทางปฏิบัติที่ดีเบื้องต้นในการเพิ่มความมั่นคงปลอดภัยให้กับแอปพลิเคชัน และระบบปฏิบัติการ

9.1. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยคลาวด์ (Cloud Security Guideline)

การประมวลผลแบบคลาวด์ (Cloud Computing) มีศักยภาพที่จะนำประโยชน์ในด้านความคล่องตัว ความยืดหยุ่นคืนสภาพได้ เศรษฐกิจ และความมั่นคงปลอดภัยให้กับผู้ใช้งานได้ ซึ่งการจะได้รับประโยชน์เหล่านี้ โดยเฉพาะด้านความมั่นคงปลอดภัย ผู้ใช้งานจะต้องมีความเข้าใจลักษณะคลาวด์ ใช้งานคลาวด์ ปรับปรุงสถาปัตยกรรม และการควบคุมให้เหมาะสมกับความสามารถ และการทำงานของคลาวด์ ถึงแม้ว่ารายละเอียดของคลาวด์ของแต่ละผู้ให้บริการจะมีความแตกต่างกัน ผู้เชี่ยวชาญได้ทำการรวบรวมกระบวนการบริหารจัดการความมั่นคงปลอดภัยของคลาวด์ในระดับสูงที่สามารถประยุกต์ใช้ได้กับคลาวด์ทั่วไป เนื้อหาในส่วนนี้ได้สรุปหลักการสำคัญ และแนวปฏิบัติที่ดีในการรักษาความมั่นคงปลอดภัยของคลาวด์เบื้องต้นสำหรับผู้ใช้บริการ ผู้ดูแลระบบ และนักพัฒนาระบบเพื่อให้สามารถใช้งานคลาวด์ได้อย่างมั่นคงปลอดภัย ทั้งนี้ ในส่วนของผู้ใช้บริการ สามารถประยุกต์ใช้ได้กับทั้งกับการใช้บริการระบบคลาวด์กลางภาครัฐ (Government Data Center and Cloud Service: GDCC) และบริการคลาวด์ของภาคเอกชน

9.1.1. ความรู้พื้นฐานเกี่ยวกับคลาวด์

สถาบันมาตรฐาน และเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology : NIST) สหรัฐอเมริกาได้ให้นิยามการประมวลผลแบบคลาวด์[1] คือ แบบจำลองสำหรับการเข้าถึงทรัพยากรการประมวลผลที่ใช้ร่วมกัน (เช่น เครือข่าย เครื่องแม่ข่าย หน่วยเก็บข้อมูล แอปพลิเคชัน และบริการ) ผ่านเครือข่ายที่สามารถเข้าถึงได้จากทุกที่ สะดวก และตามต้องการ ทรัพยากรเหล่านี้สามารถถูกจัดสรร และปล่อยคืนโดยใช้การบริหารจัดการ หรือการปฏิสัมพันธ์จากผู้ให้บริการน้อยที่สุด แบบจำลอง

[1] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

คลาวด์นี้ประกอบด้วยลักษณะสำคัญ 5 ประการ แบบจำลองบริการ (Service model) 3 แบบจำลอง และแบบจำลองการจัดเตรียมระบบ (Deployment model) 4 แบบจำลอง

9.1.2. ลักษณะสำคัญ

1) การบริการตนเองตามต้องการ (On-Demand Self-Service) ผู้ใช้บริการสามารถร้องขอ และจัดสรรทรัพยากรการประมวลผลได้ด้วยตนเองตามต้องการ โดยไม่ต้องติดต่อกับเจ้าหน้าที่ของผู้ให้บริการคลาวด์

2) การเข้าถึงผ่านเครือข่ายด้วยช่องทางที่หลากหลาย (Broad Network Access) ผู้ใช้สามารถเข้าถึงบริการผ่านระบบเครือข่ายด้วยวิธีการมาตรฐาน ผู้ใช้สามารถใช้แพลตฟอร์มเครื่องลูกข่ายที่หลากหลาย เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล สมาร์ทโฟน และแท็บเล็ต

3) การรวมทรัพยากร (Resource Pooling) ทรัพยากรการประมวลผลของผู้ให้บริการมีการรวบรวมจากหลายเครื่องแม่ข่าย และศูนย์ข้อมูลเพื่อให้บริการกับผู้ใช้บริการที่หลากหลาย โดยทั่วไปผู้ใช้บริการจะไม่รู้ตำแหน่งของทรัพยากรที่ใช้อย่างชัดเจน แต่อาจจะสามารถระบุตำแหน่งในระดับสูงได้ เช่น ประเทศ หรือศูนย์ข้อมูล

4) ความยืดหยุ่นอย่างรวดเร็ว (Rapid Elasticity) ทรัพยากรการประมวลผลสามารถถูกจัดสรรให้กับผู้ใช้ได้ตามความต้องการที่เพิ่มขึ้น หรือลด และในบางกรณีสามารถทำได้โดยอัตโนมัติเพื่อตอบสนองต่อความต้องการที่เปลี่ยนแปลงของผู้ใช้ ได้ทันท่วงที ทรัพยากรเหล่านี้อาจมีเสมือนไม่จำกัดในมุมมองของผู้ใช้

5) บริการที่วัดได้ (Measured Service) การใช้งานทรัพยากรการประมวลผลสามารถถูกวัดปริมาณ ควบคุม และรายงาน เพื่อให้ความโปร่งใสกับผู้ให้บริการ และผู้ใช้บริการ

9.1.3. แบบจำลองบริการ

1) **บริการซอฟต์แวร์ (Software as a Service)** ผู้ให้บริการให้บริการซอฟท์แวร์ที่ทำงานอยู่บนคลาวด์กับผู้ใช้งาน ผู้ใช้งานสามารถเข้าถึงบริการซอฟท์แวร์ผ่านส่วนต่อประสาน (Interface) เช่น เว็บบราวเซอร์ หรือแอปพลิเคชัน บนเครื่องลูกข่าย ผู้ใช้บริการไม่สามารถบริหารจัดการแพลตฟอร์มและโครงสร้างพื้นฐานที่ติดตั้งบริการซอฟท์แวร์ได้ ยกเว้นการตั้งค่าของบริการซอฟท์แวร์บางรายการของผู้ใช้งานนั้น ๆ

2) **บริการแพลตฟอร์ม (Platform as a Service)** ผู้ให้บริการให้บริการแพลตฟอร์มที่ผู้ใช้บริการสามารถสร้างแอปพลิเคชันต่อยอดขึ้นมาใช้งานเป็นของตนเองได้ แพลตฟอร์มนี้อาจเป็นสภาพแวดล้อมในการเขียนโปรแกรม เอนจิ้น ฐานข้อมูล ไลบรารี หรือชุดพัฒนาซอฟท์แวร์ ผู้ใช้บริการไม่สามารถบริหารจัดการโครงสร้างพื้นฐานที่ติดตั้งแพลตฟอร์มได้ ยกเว้นการตั้งค่าบางอย่างของแพลตฟอร์มสำหรับการติดตั้งและทำงานของแอปพลิเคชัน

3) **บริการโครงสร้างพื้นฐาน (Infrastructure as a Service)** ผู้ให้บริการให้บริการทรัพยากรการประมวลผล เช่น หน่วยประมวลผล หน่วยเก็บข้อมูล และเครือข่าย กับผู้ใช้งานเพื่อที่ผู้ใช้งาน

สามารถพัฒนาแอปพลิเคชัน และบริการของตนเองได้ โดยทั่วไปทรัพยากรเหล่านี้มักจะอยู่ในรูปแบบเครื่องคอมพิวเตอร์เสมือน (Virtual Machine) ผู้ใช้บริการไม่สามารถบริหารจัดการโครงสร้างพื้นฐานของคลาวด์ได้ แต่อาจสามารถบริหารจัดการ และควบคุมบางองค์ประกอบของเครือข่ายได้

9.1.4. แบบจำลองการจัดเตรียมระบบ

1) คลาวด์ส่วนตัว (Private Cloud) โครงสร้างพื้นฐานคลาวด์ถูกจัดสรรให้ใช้เฉพาะหน่วยงานใดหน่วยงานหนึ่ง โดยในหน่วยงานอาจมีผู้ใช้งานหลายคน หน่วยงาน ผู้ให้บริการภายนอก หรือหน่วยงาน และผู้ให้บริการภายนอกร่วมกันอาจเป็นเจ้าของ บริหารจัดการ และดำเนินการคลาวด์ คลาวด์อาจอยู่ภายใน หรือภายนอกพื้นที่หน่วยงานก็ได้

2) คลาวด์ชุมชน (Community Cloud) โครงสร้างพื้นฐานคลาวด์ถูกจัดสรรให้ใช้เฉพาะกลุ่มผู้ใช้จากหลายหน่วยงานที่มีความสนใจ เป้าหมาย หรือวัตถุประสงค์ร่วมกัน ความเป็นเจ้าของ การบริหารจัดการ และการดำเนินการอาจทำโดยกลุ่มหน่วยงานดังกล่าว ผู้ให้บริการภายนอก หรือร่วมกัน คลาวด์อาจอยู่ภายใน หรือภายนอกพื้นที่ของกลุ่มองค์กร

3) คลาวด์สาธารณะ (Public Cloud) โครงสร้างพื้นฐานคลาวด์เปิดให้ผู้ใช้โดยทั่วไปสามารถใช้งานได้ ความเป็นเจ้าของ การบริหารจัดการ และการดำเนินการอาจทำโดยองค์กรธุรกิจ วิชาการ หน่วยงานรัฐบาล หรือร่วมกัน คลาวด์อยู่ในพื้นที่ของผู้ให้บริการ

4) คลาวด์ผสม (Hybrid Cloud) โครงสร้างพื้นฐานคลาวด์เป็นการผสมของคลาวด์ประเภทข้างต้นที่แตกต่างกันอย่างน้อย 2 ประเภท โดยมีการเชื่อมต่อกันด้วยเทคโนโลยีมาตรฐานหรือเทคโนโลยีเฉพาะที่ช่วยให้สามารถแลกเปลี่ยนข้อมูล และแอปพลิเคชันได้

9.1.5. สำหรับผู้ใช้งานบริการคลาวด์

คลาวด์มีความแตกต่างจากโครงสร้างพื้นฐานการประมวลผลแบบเดิมที่มักจะบริหารจัดการด้วยหน่วยงานนั้น ๆ เอง เนื่องจากโครงสร้างพื้นฐานการประมวลผลแบบเดิม เช่น เซิร์ฟเวอร์ และศูนย์ข้อมูล หน่วยงานสามารถดูแล ควบคุม และตรวจสอบองค์ประกอบส่วนต่าง ๆ ของโครงสร้างพื้นฐานได้ทั้งหมด เช่น หน่วยประมวลผล หน่วยเก็บข้อมูล และเครือข่าย แต่โครงสร้างพื้นฐานการประมวลผลแบบคลาวด์ผู้ให้บริการเป็นผู้ดูแลโครงสร้างพื้นฐาน และผู้ใช้สามารถบริหารจัดการทรัพยากรได้จำกัด ความรับผิดชอบบริหารจัดการความมั่นคงปลอดภัยในแต่ละส่วนขึ้นอยู่กับประเภทบริการที่ใช้ (SaaS, PaaS, หรือ IaaS) เป็นแบบแบ่งความรับผิดชอบ (Shared Responsibility Model) เช่น บริการแบบ SaaS ผู้ใช้บริหารจัดการความมั่นคงปลอดภัยที่ระดับแอปพลิเคชัน (เช่น การจัดการบัญชีผู้ใช้ของหน่วยงาน) ส่วนผู้ให้บริการรับผิดชอบความมั่นคงปลอดภัยของแพลตฟอร์ม และโครงสร้างพื้นฐานคลาวด์ ในขณะที่บริการแบบ IaaS ผู้ใช้ต้องดูแลความมั่นคงปลอดภัยตั้งแต่ชั้นแอปพลิเคชันถึงระดับเครื่องเสมือน ส่วนผู้ให้บริการรับผิดชอบเฉพาะความมั่นคงปลอดภัยของโครงสร้างพื้นฐานคลาวด์ ส่วนประเภทของการจัดเตรียมระบบคลาวด์ เช่น คลาวด์ส่วนตัว และคลาวด์สาธารณะ จะมีผลต่อความสามารถในการควบคุมดูแลทรัพยากร และค่าใช้จ่าย ดังนั้นผู้ใช้งานควร

เลือกบริการคลาวด์ที่เหมาะสมกับความต้องการ และเข้าใจความรับผิดชอบหน้าที่ของตนเพื่อสามารถใช้งานคลาวด์ได้อย่างปลอดภัย และคุ้มค่า

คณะกรรมการการค้าของรัฐบาลกลาง (Federal Trade Commission) สหรัฐอเมริกา แนะนำ 6 ขั้นตอนในการใช้การประมวลผลแบบคลาวด์ อย่างมั่นคงปลอดภัย ดังนี้

1) ใช้ประโยชน์จากคุณสมบัติความมั่นคงปลอดภัยที่มีให้โดยผู้ให้บริการคลาวด์ ผู้ให้บริการที่ดีจะมีคู่มือรายละเอียดคุณสมบัติการควบคุมความมั่นคงปลอดภัย และวิธีการตั้งค่าการใช้งานบริการที่มีความมั่นคงปลอดภัย ผู้ใช้งานควรทำความเข้าใจกับตัวเลือก การตั้งค่า ที่เหมาะสมกับธุรกิจของผู้ใช้ ซึ่งจะต้องพิจารณาระดับความละเอียดอ่อนของข้อมูลที่จัดเก็บ และมีการใช้งานข้อมูลอย่างไร พิจารณาว่ามีใครในหน่วยงานจะต้องเข้าถึงข้อมูลใดบ้าง ใช้การพิสูจน์ตัวตนหลายปัจจัย (Multi-Factor Authentication) และรหัสผ่านที่มั่นคงปลอดภัยเพื่อลดความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาต นอกจากนี้ไม่ควรจดบันทึกรหัสผ่านไว้ในแอปพลิเคชัน หรือซอร์สโค้ดเด็ดขาด

2) สำรวจรายการทรัพย์สินที่เก็บไว้ในคลาวด์อย่างสม่ำเสมอ รายการทรัพย์สินที่เป็นปัจจุบันเป็นสิ่งจำเป็นต่อการบริหารจัดการข้อมูล ผู้ให้บริการหลายรายมีเครื่องมือ เช่น แดชบอร์ด และคอนโซลบริหารจัดการ เพื่อใช้สำหรับการบริหารจัดการสินทรัพย์ นอกจากจะต้องทราบว่าข้อมูลอะไรอยู่ที่ใดแล้ว จะต้องตรวจสอบให้มั่นใจว่าการตั้งค่าความมั่นคงปลอดภัย และสิทธิการเข้าถึงสอดคล้องกับระดับความละเอียดอ่อนของข้อมูลที่จัดเก็บ มีการทดสอบหาการตั้งค่าที่ผิดพลาด และข้อผิดพลาดของความมั่นคงปลอดภัยที่อาจทำให้เกิดความเสียหายกับข้อมูลได้ และมีการจัดเก็บไฟล์ล็อก (Log File) อย่างเหมาะสม เพื่อให้สามารถเฝ้าระวังคลาวด์ได้อย่างต่อเนื่อง

3) ไม่จัดเก็บข้อมูลส่วนบุคคลเกินจำเป็น พื้นที่จัดเก็บข้อมูลในคลาวด์อาจมีราคาที่ถูกกว่าการจัดเก็บข้อมูลในรูปแบบอื่น ๆ ทำให้ด้วยงบประมาณที่เท่ากันอาจได้พื้นที่จัดเก็บข้อมูลที่มากขึ้น โดยทั่วไปผู้ใช้งานมักจะเก็บข้อมูลที่ “อาจจะ” จำเป็นไว้ในคลาวด์เพื่อเติมเต็มพื้นที่ที่มีอยู่มาก แนวปฏิบัติที่ดีคือเก็บเฉพาะข้อมูลที่จำเป็นจริง ๆ หากข้อมูลใดไม่จำเป็นก็ไม่ควรจัดเก็บ เป็นการลดความเสี่ยงและผลกระทบจากการละเมิดข้อมูล และข้อมูลรั่วไหลได้

4) ควรเข้ารหัสลับข้อมูลที่ไม่ได้ใช้งานเป็นประจำ ข้อมูลที่จำเป็นต้องจัดเก็บแต่อาจไม่ได้ใช้งานเป็นประจำ เช่น สำรองข้อมูล ควรมีการเข้ารหัสลับเพื่อปกป้องข้อมูล โดยเฉพาะหากในสำรองข้อมูลมีข้อมูลที่ละเอียดอ่อนแล้วยิ่งควรทำการเข้ารหัสลับข้อมูล

5) ใส่ใจกับการเตือนที่น่าเชื่อถือ ผู้ให้บริการบางรายมีเครื่องมือที่มีการแจ้งเตือนผู้ใช้ถึงที่เก็บข้อมูลคลาวด์ที่ถูกเปิดให้เข้าถึงได้แบบสาธารณะ บางผู้ให้บริการอาจมีการให้เจ้าหน้าที่แจ้งกับผู้ใช้งาน นักวิจัยด้านความมั่นคงปลอดภัยอาจมีการแจ้งเตือนหน่วยงานเมื่อพบการละเมิดข้อมูลออนไลน์ หากผู้ใช้ได้รับการแจ้งเตือน ควรทำการตรวจสอบที่เก็บข้อมูล และการตั้งค่าความมั่นคงปลอดภัย

6) ความมั่นคงปลอดภัยเป็นความรับผิดชอบของผู้ใช้งาน การใช้บริการคลาวด์ไม่ได้หมายถึงการโอนถ่ายความรับผิดชอบความมั่นคงปลอดภัยให้กับผู้ให้บริการทั้งหมด ผู้ใช้งานมีความรับผิดชอบ

ต่อข้อมูลในครอบครองตลอดทั้งวงจรชีวิตของข้อมูล ถึงแม้ว่าผู้ใช้งานจะใช้เครื่องมือของผู้ให้บริการในการปกป้องความมั่นคงปลอดภัยของข้อมูล แต่ผู้ใช้งานก็ควรต้องจัดเตรียมโปรแกรม ขั้นตอน กระบวนการรักษาข้อมูล และข้อมูลละเอียดอ่อนต่าง ๆ ผู้ใช้งานในหน่วยงานควรมีความรู้ และความสามารถที่จำเป็นในการดำเนินการรักษา ตรวจสอบ ทดสอบ และปรับปรุงโปรแกรม ขั้นตอน และกระบวนการเหล่านั้นได้ ผู้ใช้งานควรมีการทบทวนสัญญาการใช้บริการกับผู้ให้บริการอย่างละเอียดถี่ถ้วนเพื่อให้เข้าใจชัดเจนถึงขอบเขตความรับผิดชอบของแต่ละฝ่าย ทั้งนี้ควรระลึกไว้เสมอว่าผู้ใช้งานเป็นผู้มีความรับผิดชอบสูงสุดต่อข้อมูลในครอบครอง

นอกจากคำแนะนำโดยคณะกรรมการการค้าของรัฐบาลกลางข้างต้นแล้ว หน่วยงานควรพิจารณาข้อแนะนำเพิ่มเติมดังนี้

1) ควรมีการสำรองข้อมูล และทดสอบการกู้คืนข้อมูล เพื่อที่จะสามารถกู้คืนข้อมูลได้ทันท่วงทีเมื่อเกิดเหตุการณ์ทำให้ข้อมูลเสียหาย

2) ควรเลือกคลาวด์จากผู้ให้บริการที่สามารถนำออกระบบ และข้อมูล และย้ายไปยังคลาวด์อื่นได้สะดวก คลาวด์ที่มีระบบเฉพาะ และไม่ได้ใช้มาตรฐานที่เป็นที่ยอมรับโดยทั่วไปอาจทำให้เกิดปัญหาการล็อคติดกับผู้ให้บริการ (Vendor Lock-in) ได้

3) ควรเตรียมแผนการตอบสนองต่อเหตุการณ์ไม่คาดคิด และแผนความต่อเนื่องของการดำเนินธุรกิจ เนื่องจากทุกระบบคลาวด์ถือว่ามีความเสี่ยงที่อาจจะเกิดเหตุการณ์ไม่คาดคิด ถูกโจมตี ผู้ให้บริการยุติการให้บริการ หรือเหตุการณ์อื่น ๆ ทำให้ไม่สามารถใช้บริการคลาวด์อย่างต่อเนื่องได้ หน่วยงานจึงควรเตรียมแผนการตอบสนองต่อเหตุการณ์ไม่คาดคิด และแผนความต่อเนื่องของการดำเนินธุรกิจเพื่อเป็นแนวปฏิบัติรับมือกรณีที่คลาวด์ไม่สามารถใช้งานได้ นอกจากนี้ยังควรมีการซักซ้อมตามแผน ทบทวน และตรวจสอบแผนเป็นประจำ

4) ควรมีการประเมินการจัดเตรียมระบบ และมาตรการควบคุมความมั่นคงปลอดภัยของคลาวด์ เพื่อตรวจสอบว่าคลาวด์นั้น ๆ ปฏิบัติตามแนวทางที่ดี มีมาตรการควบคุมความมั่นคงปลอดภัยที่เหมาะสม และเข้าใจว่าแต่ละฝ่ายควรดูแลความมั่นคงปลอดภัยในส่วนใด โดยหนึ่งในแนวทางที่เป็นที่ยอมรับคือ Cloud Controls Matrix (CCM) ที่ถูกพัฒนาโดย Cloud Security Alliance (CSA)

9.1.6. สำหรับผู้ดูแลระบบ

ผู้ดูแลระบบควรดำเนินการรักษาความมั่นคงปลอดภัยของคลาวด์ในส่วนที่ผู้ใช้ทั่วไปไม่สามารถเข้าถึงได้ โดยควรดูแลความมั่นคงปลอดภัยของโครงสร้างพื้นฐานคลาวด์ (รวมถึงเครือข่ายและแพลตฟอร์มที่ให้บริการผู้ใช้งาน) และการบริหารจัดการอัตลักษณ์ และการเข้าถึง (Identity and Access Management) ผู้ดูแลระบบอย่างน้อยควรคำนึงถึงสิ่งต่อไปนี้

1) ใช้หลักการสิทธิพิเศษขั้นต่ำ (Least Privilege) ซึ่งเป็นการให้สิทธิการเข้าถึงระบบและข้อมูลกับผู้ใช้น้อยที่สุดเท่าที่จำเป็นในการปฏิบัติงานของผู้ใช้

2) ใช้การพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย หากมีการใช้รหัสผ่านก็ควรมีการใช้รหัสผ่านที่มีความมั่นคงปลอดภัย ยากต่อการคาดเดา และเป็นไปตามแนวปฏิบัติการใช้รหัสผ่านที่ดี

เช่น แนวปฏิบัติโดยสถาบันมาตรฐาน และเทคโนโลยีแห่งชาติ[2] สำหรับระบบ และข้อมูลที่สำคัญควรพิจารณาใช้การพิสูจน์ตัวตนหลายปัจจัยเพื่อลดความเสี่ยงจากการเข้าถึงระบบโดยไม่ได้รับอนุญาต ทั้งนี้ควรมีการศึกษาพฤติกรรมของผู้ใช้ด้วย หากมีการบังคับใช้วิธีการที่ไม่เหมาะสมกับบริบท อาจทำให้ผู้ใช้หาวิธีหลบเลี่ยง หรือใช้ปัจจัยการพิสูจน์ตัวตนที่ไม่มั่นคงปลอดภัยได้

3) ใช้เครื่องมือบริหารจัดการอัตลักษณ์ และการเข้าถึงอย่างเหมาะสม เพื่อใช้ในการบริหารจัดการบัญชีผู้ใช้ สิทธิการเข้าถึง และอื่น ๆ ที่เกี่ยวข้อง

4) มีการตรวจสอบ และเฝ้าระวังการเข้าใช้งานระบบ มีการเฝ้าระวังบันทึกกิจกรรมการเข้าใช้งานของผู้ใช้ และความพยายามในการเข้าถึงเพื่อตรวจสอบกิจกรรมที่น่าสงสัย และอาจเป็นอันตราย

5) ใช้การตั้งค่าคลาวด์ที่มีความมั่นคงปลอดภัย โดยตั้งค่าคลาวด์ให้มีความมั่นคงปลอดภัยตามแนวปฏิบัติที่ดีเพื่อลดช่องโหว่ความมั่นคงปลอดภัย

6) ติดตั้งแพทช์ และปรับให้ซอฟท์แวร์เป็นปัจจุบันอยู่เสมอ ดูแลรักษาให้ซอฟท์แวร์มีการติดตั้งแพทช์ และปรับปรุงให้เป็นปัจจุบันอยู่เสมอ เพื่อแก้ไขช่องโหว่ความมั่นคงปลอดภัยที่ถูกค้นพบ และได้รับการแก้ไขแล้ว และลดความเสี่ยงจากการใช้ประโยชน์จากช่องโหว่เพื่อเข้าสู่ระบบ และข้อมูลโดยไม่ได้รับอนุญาต

7) ติดตั้งการควบคุมความมั่นคงปลอดภัยอย่างเหมาะสม ควรมีการเลือกใช้ และติดตั้งให้เหมาะสมในบริบทของคลาวด์ ตัวอย่างเช่น การใช้ไฟร์วอลใน บริบทคลาวด์จะมีความแตกต่างจากระบบเครือข่ายแบบดังเดิมที่เครือข่ายเชื่อมต่อระหว่างเครื่องต่าง ๆ มีการแยกออกจากกัน และมีขอบเขตที่ค่อนข้างชัดเจน ในขณะที่แอปพลิเคชันบนคลาวด์อาจมีการเชื่อมต่อกับหน่วยต่าง ๆ ที่อยู่บนเครื่องเดียวกัน หรือต่างเครื่อง ไฟร์วอลแบบดั้งเดิมอาจไม่สามารถควบคุมการส่งข้อมูลต่าง ๆ เหล่านี้ได้

8) มีการบันทึกล็อก และเฝ้าระวัง เก็บบันทึกกิจกรรมของระบบ และเหตุการณ์ความมั่นคงปลอดภัยอย่างเหมาะสมเพื่อใช้ในการวิเคราะห์ และตอบสนองต่อเหตุการณ์ไม่คาดคิด

9) มีการทดสอบ และทบทวนการควบคุมความมั่นคงปลอดภัยอย่างสม่ำเสมอ รวมถึงการสแกนช่องโหว่ความมั่นคงปลอดภัย และการทดสอบเจาะระบบเพื่อค้นหา และแก้ไขช่องโหว่ความมั่นคงปลอดภัย ควรตรวจสอบเป็นประจำว่าการควบคุมความมั่นคงปลอดภัยต่าง ๆ เช่น ไฟร์วอล IDS และโปรแกรมต่อต้านซอฟท์แวร์ไม่พึงประสงค์ ยังทำงานได้ตามปกติ หรือไม่ ทบทวนว่าการควบคุมใดยังมีผล หรือจำเป็นต้องปรับปรุง หรือเพิ่มเติม หรือไม่

10) มีการฝึกอบรมผู้ดูแลระบบคลาวด์สม่ำเสมอ เพื่อเสริมสร้างความรู้ และเตรียมความพร้อมผู้ดูแลระบบให้รู้ทันภัยคุกคามใหม่ ๆ และการรับมือภัยคุกคาม และปฏิบัติตามแนวทางปฏิบัติที่ดีที่มีการปรับปรุงให้ทันสมัย

[2] https://pages.nist.gov/800-63-3/sp800-63b.html

9.1.7. สำหรับนักพัฒนาระบบ

นักพัฒนาระบบควรปฏิบัติตามแนวทางการเขียนโค้ดที่มั่นคงปลอดภัย (Secure Coding Practice) ใช้คุณลักษณะของคลาวด์อย่างเหมาะสม และพัฒนาซอฟท์แวร์ให้ตรงกับสถาปัตยกรรมของคลาวด์ เพื่อใช้ประโยชน์จากคลาวด์ให้ได้มากที่สุด และมีความมั่นคงปลอดภัย นักพัฒนาระบบควรคำนึง

1) มีการออกแบบซอฟท์แวร์ให้มีความมั่นคงปลอดภัย มีการเก็บรวบรวมความต้องการของผู้ใช้ สร้างแบบจำลองภัยคุกคาม (Threat Model) ออกแบบสถาปัตยกรรมให้เหมาะสมมั่นคงปลอดภัย

2) มีการทดสอบความมั่นคงปลอดภัยตลอดวงจรชีวิตการพัฒนาซอฟท์แวร์ เช่น Static Test, Code Review, Dynamic Test, และ Unit Test ไม่ใช่ทำเฉพาะการตรวจสอบช่องโหว่และการทดสอบเจาะระบบเพียงอย่างเดียว และควรมีการทดสอบเป็นประจำ อย่างน้อยเมื่อมีการประกาศการพบช่องโหว่ใหม่ และเมื่อซอฟท์แวร์มีการเปลี่ยนแปลง

3) มีการตรวจสอบข้อมูลที่นำเข้าจากผู้ใช้ มีการตรวจสอบข้อมูลที่นำเข้าจากผู้ใช้ทั้งฝั่งเครื่องลูกข่าย และเครื่องแม่ข่าย และทำความสะอาดข้อมูลก่อนนำข้อมูลไปประมวลผลต่อ เพื่อลดความเสี่ยงจากการถูกโจมตีต่าง ๆ เช่น SQL injection และ Cross-Site Scripting (XSS)

4) ใช้ไลบรารี และเฟรมเวิร์คที่น่าเชื่อถือ และมีความมั่นคงปลอดภัย เลือกใช้ไลบรารีและเฟรมเวิร์คที่เป็นที่ยอมรับ มีประวัติการรักษาความมั่นคงปลอดภัยที่ดี และมีการปรับปรุงซอฟท์แวร์เพื่อแก้ไขช่องโหว่ความมั่นคงปลอดภัยอย่างสม่ำเสมอ

5) มีการเข้ารหัสลับข้อมูลที่มีความละเอียดอ่อน ข้อมูลสำคัญ และข้อมูลละเอียดอ่อนควรได้รับการเข้ารหัสลับทั้งขณะที่จัดเก็บ (Data at Rest) และขณะที่อยู่ระหว่างส่งผ่านเครือข่าย (Data in Transit) เลือกใช้ระบบรหัสลับที่มีความมั่นคงปลอดภัย เป็นที่ยอมรับ ได้มาตรฐาน และปรับปรุงทดแทนระบบรหัสลับที่มีการค้นพบช่องโหว่ความมั่นคงปลอดภัย

6) ลดพื้นที่การโจมตี เขียนโค้ดให้กระชับ และมีเฉพาะฟังก์ชันที่มีความจำเป็นต่อการทำงานของซอฟท์แวร์เท่านั้น เพื่อลดความเสี่ยงจากการถูกโจมตีผ่านช่องโหว่ซอฟท์แวร์

7) ตั้งค่าสภาพแวดล้อม และการใช้งานคลาวด์ให้มั่นคงปลอดภัย ปฏิบัติตามแนวทางการตั้งค่าที่มีความมั่นคงปลอดภัยที่แนะนำโดยผู้ให้บริการ และมีการกำหนดสิทธิการเข้าถึงอย่างเหมาะสม

8) บริหารจัดการความลับ (Secret) อย่างมั่นคงปลอดภัย ใช้กระบวนการที่มีความมั่นคงปลอดภัย เช่น ระบบบริหารจัดการกุญแจรหัสลับ ในการจัดเก็บ และบริหารจัดการข้อมูลลับ เช่น กุญแจรหัสลับของ API และ รหัสผ่าน

9) ใช้เครื่องมือในการเฝ้าระวังภัยคุกคาม ใช้เครื่องมือของคลาวด์ในการตรวจสอบและเฝ้าระวังภัยคุกคาม และช่องโหว่ความมั่นคงปลอดภัย

10) มีการฝึกอบรมนักพัฒนาระบบสม่ำเสมอ เพื่อเสริมสร้างความรู้ และเตรียมความพร้อมนักพัฒนาระบบให้รู้ทันภัยคุกคามใหม่ ๆ และการรับมือภัยคุกคาม และปฏิบัติตามแนวทางปฏิบัติที่ดีที่มีการปรับปรุงให้ทันสมัย

11) มีการออกแบบซอฟท์แวร์ให้เหมาะสมกับคุณลักษณะของคลาวด์ เช่น การออกแบบสถาปัตยกรรมซอฟท์แวร์เป็นแบบ Microservice ที่แบ่งหน่วยการประมวลแยกย่อยตามฟังก์ชันการทำงานของระบบ ลดการพึ่งพากันอย่างเหนียวแน่นระหว่างฟังก์ชัน เพื่อรองรับการปรับขยายตัวเพิ่มขึ้น หรือลดลงตามปริมาณผู้ใช้งาน นอกจากนี้ผลกระทบจากปัญหาการทำงานของบางฟังก์ชันอาจลดผลกระทบต่อฟังก์ชันอื่น ๆ และสามารถแก้ไขได้โดยการปรับปรุงเฉพาะหน่วยประมวลผล และเริ่มต้นการทำงานใหม่

12) มีการทำ Immutable Workload หรือการทำ Template หรือ Gold Master ที่เป็นต้นฉบับของแอปพลิเคชัน หรือฟังก์ชัน เมื่อนำไปใช้งานแล้วผู้ใช้จะไม่สามารถทำการแก้ไขต่อระบบที่เริ่มมาจากต้นฉบับได้ หรือการแก้ไขจะไม่ส่งผลกระทบ หรือถูกบันทึกกลับคืนไปยังต้นฉบับ การใช้ Immutable Workload มีประโยชน์คือการแก้ไขที่อาจจะทำให้เกิดปัญหากับระบบจะไม่ส่งผลกระทบกับต้นฉบับ และเมื่อต้องการทำการปรับปรุงแก้ไขระบบ สามารถปรับแก้ที่ต้นฉบับ หยุดการทำงานของระบบเดิม และเริ่มระบบจากต้นฉบับใหม่ได้อย่างรวดเร็ว

13) ควรมีกระบวนการจัดเก็บกิจกรรม และเหตุการณ์ที่เกิดขึ้นกับแอปพลิเคชัน ลงในไฟล์ล็อกที่ระดับแอปพลิเคชัน และจัดเก็บอย่างเหมาะสม เนื่องจากนักพัฒนาระบบอาจจะไม่สามารถเข้าถึงล็อกของระบบปฏิบัติการ เครือข่าย หรือล็อกอื่น ๆ ได้เหมือนกับโครงสร้างพื้นฐานแบบดั้งเดิม ดังนั้นผู้พัฒนาควรมีการเก็บข้อมูลลงในไฟล์ล็อกที่ระดับแอปพลิเคชันเพื่อใช้ในการวิเคราะห์ และเฝ้าระวัง

14) ลดการพึ่งพาการอ้างอิง และเข้าถึงด้วย IP Address เนื่องจากเครื่องเสมือนและหน่วยทำงานในคลาวด์อาจจะมีการเคลื่อนย้ายไปยังเครื่องกายภาพอื่น ๆ ในคลาวด์ได้โดยที่นักพัฒนาระบบอาจจะไม่สามารถควบคุมได้ ทำให้อาจมีการเปลี่ยนแปลงของ IP Address ควรใช้การอ้างอิงอื่น ๆ ที่รองรับการเปลี่ยนแปลงตำแหน่ง และการเคลื่อนย้ายของเครื่องเสมือน และหน่วยทำงานได้

การเลือกใช้งานคลาวด์หลายที่หรือ Multi-cloud

ในบางกรณีผู้ใช้หรือหน่วยงานอาจมีการพิจารณาเลือกใช้ Multi-cloud ซึ่งก็คือการใช้ระบบที่ติดตั้งบนคลาวด์ที่ให้บริการโดยผู้ให้บริการตั้งแต่ 2 รายขึ้นไป อาจจะเป็นการผสมระหว่างคลาวด์สาธารณะหลายที่หรือคลาวด์ส่วนตัวและคลาวด์สาธารณะก็ได้ เพื่อตอบสนองความต้องการของธุรกิจอย่างเหมาะสม เหตุผลหลักที่อาจเลือกใช้งานคลาวด์หลายที่มีดังนี้

1. สามารถเลือกใช้งานคลาวด์จากผู้ให้บริการคลาวด์หลายรายที่มีลักษณะเหมาะสมกับความต้องการเฉพาะแต่ละส่วน เช่น ความเร็วในการประมวลผล ความพร้อมใช้งาน ตำแหน่งที่ตั้ง และการปฏิบัติตามกฎ ระเบียบ และข้อบังคับ เป็นต้น
2. การเลือกใช้งานคลาวด์หลายที่เป็นการลดการพึ่งพาผู้ให้บริการรายใดรายหนึ่งมากจนเกินไป ซึ่งหากมีการพึ่งพาผู้ให้บริการเพียงรายเดียวมากเกินไปอาจทำให้ต้นทุนในการย้ายระบบและข้อมูลเมื่อจำเป็นสูงมากได้

3. ผู้ใช้สามารถเลือกผู้ให้บริการที่มีค่าบริการและการให้บริการที่เหมาะสม คุ้มค่ากับความต้องการได้ เช่น การเลือกบริการการประมวลผลจากผู้ให้บริการรายหนึ่งและบริการเก็บข้อมูลจากผู้ให้บริการอีกรายหนึ่ง

4. การใช้งานคลาวด์หลายที่ลดความเสี่ยงและผลกระทบจากการขัดข้องของระบบของผู้ให้บริการรายใดรายหนึ่ง ถึงแม้ว่าจะมีคลาวด์จากผู้ให้บริการรายหนึ่งไม่พร้อมใช้งาน ผู้ใช้ยังสามารถใช้บริการจากผู้ให้บริการรายอื่น ๆ ได้ เป็นการกระจายความเสี่ยงที่ดี

ทั้งนี้ การเลือกใช้งานคลาวด์หลายที่มีความท้าทายและข้อที่ควรต้องคำนึงดังต่อไปนี้

1. ความซับซ้อนในการออกแบบ บริหารจัดการ และการดูแลระบบ เนื่องจากระบบมีการเชื่อมต่อกับองค์ประกอบที่อยู่บนคลาวด์หลายที่ซึ่งมักจะเพิ่มความซับซ้อนของระบบ

2. ความแตกต่างของระดับการรักษาความมั่นคงปลอดภัยคลาวด์ของแต่ละผู้ให้บริการอาจมีมาตรการและระดับการรักษาความมั่นคงปลอดภัยที่แตกต่างกันผู้ใช้งานควรศึกษาการรักษาความมั่นคงปลอดภัยของแต่ละผู้ให้บริการอย่างถี่ถ้วน และหามาตรการในการลดช่องโหว่ความมั่นคงปลอดภัยที่อาจเกิดขึ้นจากความไม่สอดคล้องของระดับการรักษาความมั่นคงปลอดภัยของแต่ละผู้ให้บริการ

3. การเลือกใช้มาตรฐานในการแลกเปลี่ยนข้อมูลและการเชื่อมต่อขององค์ประกอบระหว่างคลาวด์จะต้องรองรับโดยคลาวด์ของแต่ละผู้ให้บริการมาตรฐานที่ใช้เฉพาะบนคลาวด์ของผู้ให้บริการรายหนึ่งอาจไม่รองรับโดยคลาวด์ของผู้ให้บริการรายอื่น ทำให้ไม่สามารถแลกเปลี่ยนข้อมูลและเชื่อมต่อได้

4. ผู้ใช้ควรศึกษาว่าการใช้คลาวด์ของแต่ละผู้ให้บริการยังเป็นไปตามการปฏิบัติตามกฎ ระเบียบ และข้อบังคับที่เกี่ยวข้องหรือไม่

5. ควรมีการออกนโยบายและแนวปฏิบัติที่ชัดเจนในการใช้งานระบบที่อยู่บนคลาวด์หลายที่เพื่อให้มั่นใจว่าผู้ใช้งานสามารถใช้งานได้อย่างมั่นคงปลอดภัยนโยบายและแนวปฏิบัติรวมถึงการควบคุมการเข้าถึง การเฝ้าระวังภัยคุกคาม และการปฏิบัติตามกฎ ระเบียบ และข้อบังคับที่เกี่ยวข้อง

6. ควรเลือกใช้เครื่องมือในการบริการจัดการทรัพยากรของแต่ละคลาวด์อย่างเหมาะสมสามารถบริหารจัดการแบบรวมศูนย์และแสดงข้อมูลที่เป็นประโยชน์ได้อย่างชัดเจน สะดวก รวดเร็ว

ตัวอย่างหัวข้อสัญญาบริการคลาวด์

สัญญาบริการคลาวด์เป็นเอกสารที่ร่างขึ้นเพื่อระบุข้อตกลงการให้และรับบริการคลาวด์ระหว่างผู้ให้บริการคลาวด์และผู้รับบริการคลาวด์ เพื่อช่วยให้ทั้งสองฝ่ายมีความเข้าใจต่อความต้องการ หน้าที่และความรับผิดชอบของตนเอง ป้องกันการขัดแย้งและช่วยแก้ปัญหาเมื่อมีข้อพิพาทเกิดขึ้น ในสัญญาควรมีการระบุรายละเอียดที่ผู้รับบริการคลาวด์ต้องการจากผู้ให้บริการคลาวด์เพื่อให้ผู้ให้บริการสามารถให้บริการได้อย่างมีคุณภาพตามที่ผู้รับบริการคลาวด์คาดหวัง มีการระบุเงื่อนไขและภาระรับผิดชอบทั้งฝ่ายผู้ให้บริการคลาวด์ และฝ่ายผู้รับบริการคลาวด์ในกรณีที่ฝ่ายใดฝ่ายหนึ่งไม่สามารถปฏิบัติตามข้อตกลงที่ระบุในสัญญาได้ รวมถึงมีการระบุการคิดค่าใช้จ่ายของบริการอย่างชัดเจน และมีวิธีวัดคุณภาพของบริการอย่างเป็นรูปธรรม โดยในสัญญาควรมีหัวข้อเบื้องต้น ดังต่อไปนี้

1. **วัตถุประสงค์ของสัญญา** มีการระบุเจตนาของการทำสัญญาโดยภาพรวม อธิบายวัตถุประสงค์ของการบริการ

2. **ขอบเขตของการบริการ** มีการระบุสิ่งที่ผู้รับบริการคาดหวังและสิ่งที่ให้บริการจะต้องปฏิบัติตามข้อตกลงและเงื่อนไขที่กำหนดไว้

3. **ประสิทธิภาพการให้บริการ** มีการระบุประสิทธิภาพที่ผู้รับบริการต้องการตามความจำเป็นและเหมาะสม หากมีการกำหนดคุณภาพที่สูงเกินไปก็อาจมีค่าใช้บริการที่สูงเกินไป หากมีการกำหนดคุณภาพที่ต่ำเกินไปก็อาจมีผลกระทบต่อการใช้บริการและการดำเนินกิจการของผู้รับบริการได้ ประเด็นสำคัญที่ควรมีการระบุไว้ในสัญญามีดังนี้

- Uptime คือระยะเวลาที่ระบบคลาวด์พร้อมใช้งาน และทำงานเป็นปกติ มักมีการระบุเป็นเปอร์เซ็นต์ เช่น 97%, 99.5%, หรือ 99.95% เนื่องจากระบบคลาวด์อาจเกิดความขัดข้องหรือต้องได้รับการบำรุงรักษาทำให้ไม่สามารถให้บริการได้ตลอดเวลาทั้งเดือนหรือทั้งปี
- Throughput คือความเร็วในการส่งถ่ายข้อมูลจากที่หนึ่งไปยังอีกที่หนึ่งในระยะเวลาที่กำหนด
- Response time คือระยะเวลาตั้งแต่ผู้ใช้บริการคลาวด์ส่งคำร้องขอเข้าถึงทรัพยากรจนถึงระยะเวลาที่คลาวด์จัดสรรและส่งทรัพยากรที่ผู้ใช้ร้องขอมาให้
- Concurrent user คือจำนวนผู้ใช้ที่สามารถเข้าใช้บริการคลาวด์ได้พร้อมกันในช่วงระยะเวลาใดเวลาหนึ่ง

นอกจากนี้อาจมีการระบุมาตฐานหรือการรับรองที่ผู้ให้บริการควรมีเพื่อให้มั่นใจถึงคุณภาพในการให้บริการกับผู้รับบริการได้

4. **มาตรการการแก้ไขปัญหา** มีการระบุวิธีการแก้ปัญหาเมื่อเกิดปัญหาขึ้น เช่น ไม่สามารถเข้าถึงบริการคลาวด์ได้ บริการคลาวด์ขัดข้อง ข้อมูลสูญหาย การประมวลผลผิดพลาด หรือแม้กระทั่งการเกิดความเสียหายจากภัยคุกคามทางไซเบอร์ นอกจากนี้ยังควรกำหนดระยะเวลาในการแก้ปัญหาแต่ละเรื่องในแต่ละครั้ง ทั้งนี้ผู้ใช้บริการคลาวด์อาจต้องมีความรับผิดชอบร่วมด้วยในบางส่วน เช่น ผู้ใช้บริการคลาวด์จะต้องมีการฝึกอบรมเพื่อใช้บริการคลาวด์อย่างถูกต้องเหมาะสม ทำตามขั้นตอนที่ถูกต้อง ไม่ใช้บริการคลาวด์นอกเหนือจากวัตถุประสงค์ที่ได้ระบุไว้ และดูแลรักษาความมั่นคงปลอดภัยในส่วนของผู้ใช้บริการ เช่น การจัดการบัญชีผู้ใช้ อย่างเหมาะสม

5. **ค่าบริการ** มีการระบุค่าใช้บริการคลาวด์ในแต่ละรายการ วิธีการคิด และเงื่อนไขการชำระเงินให้ชัดเจน

6. **หน้าที่ของผู้ใช้บริการ** มีการระบุหน้าที่ส่วนที่ผู้ใช้บริการต้องรับผิดชอบขึ้นอยู่กับชนิดของงานและประเภทบริการของคลาวด์ที่ใช้ เช่น IaaS, PaaS, หรือ SaaS นอกจากนี้ ผู้ใช้บริการควรให้ความร่วมมือกับผู้ให้บริการในการให้ข้อมูลเกี่ยวกับการใช้บริการอย่างสม่ำเสมอเพื่อใช้ในการปรับปรุงบริการอย่างมีคุณภาพ

7. การรับประกัน มีการระบุการรับประกันคุณภาพบริการ มาตรการแก้ปัญหา และการรักษาความมั่นคงปลอดภัย หากผู้ให้บริการไม่สามารถทำตามข้อตกลงที่ระบุในสัญญาได้ก็จะมีบทปรับ ผู้ใช้บริการควรมีการเจรจากับผู้ให้บริการเพื่อให้เกิดข้อตกลงร่วมกันอย่างเหมาะสม

8. ความมั่นคงปลอดภัย มีการระบุหน้าที่ความรับผิดชอบของผู้ให้บริการว่าจะต้องมีมาตรการรักษาความมั่นคงปลอดภัยในส่วนใดบ้าง และหน้าที่ความรับผิดชอบของผู้ใช้บริการที่ต้องดูแลในส่วนตนเอง นอกจากนี้ผู้ให้บริการควรมีคู่มือ แนวปฏิบัติ และเครื่องมือให้กับผู้ใช้บริการเพื่อทำการเสริมสร้างความมั่นคงปลอดภัยบริการคลาวด์ที่ใช้อย่างเหมาะสม

9. การปฏิบัติตามระเบียบและกฎหมาย มีการระบุว่าผู้ใช้บริการมีความต้องการใดเพื่อเป็นการปฏิบัติตามกฎ ระเบียบ หรือข้อบังคับที่ผู้ใช้บริการต้องปฏิบัติตาม เช่น การดูแลรักษาข้อมูลไม่ให้รั่วไหลสู่ภายนอก ผู้ให้บริการควรระบุรายละเอียดและวิธีการที่ช่วยให้เป็นไปตามกฎ ระเบียบ หรือข้อบังคับดังกล่าว รวมถึงมาตรการในการแก้ไขเมื่อเกิดเหตุไม่พึงประสงค์ขึ้น

10. การรักษาความลับของข้อมูลและทรัพย์สินทางปัญญา มีการระบุหน้าที่ของทั้งสองฝ่ายจะต้องไม่เปิดเผยความลับข้อมูลและไม่ละเมิดทรัพย์สินทางปัญญาของแต่ละฝ่าย ในกรณีที่ผู้ให้บริการจำเป็นต้องให้บริการผ่านบุคคลที่สาม ผู้ให้บริการจะต้องกำหนดวิธีและมาตรการในการรักษาความลับข้อมูลและทรัพย์สินทางปัญญาอย่างชัดเจน

11. การป้องกันความรับผิด (Liability Protection) เนื่องจากผู้ให้บริการคลาวด์อาจมีการติดตั้งระบบคลาวด์ให้ทำงานอยู่ในหลายประเทศ ข้อมูลที่นำเข้าสู่ระบบคลาวด์อาจถูกจัดสรรการประมวลในคลาวด์ที่ตั้งอยู่ในประเทศต่าง ๆ โดยอัตโนมัติ บางประเทศอาจมีข้อห้ามในการประมวลผลข้อมูลบางประเภท ทำให้ผู้ให้บริการอาจถูกสั่งห้ามไม่ให้ประมวลผลจากบางประเทศ เป็นเหตุให้การให้บริการไม่สามารถดำเนินการต่อไปได้ ดังนั้นผู้ใช้บริการควรมีการศึกษาร่วมกับผู้ให้บริการล่วงหน้าก่อนเริ่มใช้บริการ และระบุอย่างชัดเจนการป้องกันความรับผิดในกรณีที่เกิดปัญหาดังกล่าวขึ้น

12. การทบทวนสัญญา เนื่องจากบริการคลาวด์มีโอกาสพัฒนาและปรับปรุงฟังก์ชันความสามารถต่าง ๆ ที่ดีขึ้นได้ เพื่อประโยชน์ของผู้ใช้บริการ ถ้าจำเป็นต้องมีการปรับปรุงเปลี่ยนแปลงแนวทางการใช้บริการให้เหมาะสมมากขึ้น สัญญาควรเปิดโอกาสให้ปรับปรุงแก้ไขได้ตามสถานการณ์และความจำเป็น

13. การยกเลิกสัญญา มีการระบุช่องทางและวิธีปฏิบัติให้ทั้งสองฝ่ายสามารถบอกเลิกสัญญากับอีกฝ่ายได้ ทั้งนี้ควรมีการกำหนดข้อตกลงเกี่ยวกับความเป็นเจ้าของข้อมูลอย่างชัดเจน รวมถึงขั้นตอนและกระบวนการการนำออกข้อมูลคืนให้กับผู้ใช้บริการหรือย้ายไปยังระบบใหม่ และระยะเวลาที่ต้องดำเนินการให้แล้วเสร็จ

14. การดำเนินการ มีการระบุแผนงานและตารางเวลาตั้งแต่วันที่โอนย้ายงานจากระบบเดิมไปสู่บริการคลาวด์จนถึงวันที่พร้อมให้บริการกับผู้ใช้ได้ ควรมีการกำหนดสิ่งส่งมอบที่สำคัญตลอดช่วงเวลาการทำงานตลอดสัญญา และการตรวจรับสิ่งส่งมอบโดยผู้รับบริการว่าตรงตามข้อตกลงที่ระบุในสัญญาหรือไม่ และออกหลักฐานการตรวจรับให้กับผู้ให้บริการ

15. การจ้างช่วง ในกรณีที่ผู้ให้บริการจำเป็นต้องมีการจ้างช่วงต่อกับบุคคลที่สามและผู้ใช้บริการไม่ขัดข้อง ผู้ให้บริการจะต้องมีการทำสัญญาหรือกำหนดข้อตกลงกับผู้ที่รับจ้างช่วงให้ดำเนินการในส่วนที่เกี่ยวข้องเพื่อปฏิบัติตามข้อตกลงที่ระบุในสัญญา เช่น จะต้องมีมาตรการการรักษาความลับข้อมูลอย่างเข้มงวดและเหมาะสม หากเกิดปัญหาผู้ให้บริการจำเป็นจะต้องรับผิดชอบในความเสียหายที่เกิดขึ้น และอาจไปเรียกร้องความรับผิดชอบกับผู้รับจ้างช่วง

16. การติดต่อและการแจ้งเตือน มีการระบุช่องทาง วิธีการ และผู้ประสานงานติดต่อของทั้งสองฝ่ายเพื่อให้สามารถติดต่อประสานงานในกรณีต่าง ๆ ได้หากมีการเปลี่ยนแปลงช่องทาง วิธีการ ผู้ประสานงานหรือข้อมูลอื่นที่เกี่ยวข้อง จะต้องมีการแจ้งอีกฝ่ายโดยไม่ชักช้า

17. การลบข้อมูลหลังหมดสัญญา มีการระบุมาตรการ วิธีการ และระยะเวลาในการลบทำลายข้อมูลของผู้ใช้บริการหลังจากสัญญาสิ้นสุดลง เพื่อปฏิบัติตามกฎ ระเบียบ ข้อบังคับที่เกี่ยวข้องและลดความเสี่ยงการเกิดการละเมิดและรั่วไหลของข้อมูลของผู้ใช้บริการ

สำหรับผู้ที่สนใจรายละเอียดเกี่ยวกับแนวปฏิบัติที่ดีในการใช้งานคลาวด์อย่างมีความมั่นคงปลอดภัย สามารถศึกษาข้อมูลเพิ่มเติมได้จากแหล่งข้อมูล และเอกสารดังต่อไปนี้

- Six steps toward more secure cloud computing, FTC, https://www.ftc.gov/business-guidance/blog/2020/06/six-steps-toward-more-secure-cloud-computing
- Cloud Controls Matrix and CAIQ v4, CSA https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4
- Security Guidance for Critical Areas of Focus in Cloud Computing, CSA, https://cloudsecurityalliance.org/research/guidance
- Google Cloud security best practices center, Google Cloud, https://cloud.google.com/security/best-practices
- 16 Cloud security best practices, Crowdstrike, https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-best-practices/

9.2. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยสำหรับส่วนต่อประสานโปรแกรมประยุกต์ (API Security Guideline)

Application Programming Interface (API) หรือ ส่วนต่อประสานโปรแกรมประยุกต์ เป็นเซ็ทของข้อกำหนด หรือโปรโตคอลที่ช่วยให้แอปพลิเคชันต่าง ๆ สามารถเชื่อมต่อแลกเปลี่ยนข้อมูล และบริการได้ API เปรียบเสมือนเป็นชั้นกลางที่ทำการรับส่งข้อมูลระหว่างระบบ ช่วยให้นักพัฒนาระบบสามารถพัฒนาระบบได้มีประสิทธิภาพมากขึ้น เชื่อมต่อข้อมูล และบริการได้สะดวก และยังช่วยหน่วยงานสามารถเปิดข้อมูลและบริการให้กับนักพัฒนาระบบภายใน และภายนอกหน่วยงานได้อีกด้วย

API มีการใช้งานที่หลากหลายไม่ว่าจะเป็นการแลกเปลี่ยนข้อมูลระหว่าง แอปพลิเคชันในเครื่องเดียวกัน หรือแอปพลิเคชันที่อยู่ห่างไกลผ่านระบบเครือข่าย API สามารถแบ่งตามประเภทการใช้งานได้เป็น

Public API เป็น API ที่หน่วยงานเปิดสู่สาธารณะให้ผู้ใช้ภายนอกสามารถใช้บริการได้ ทั้งนี้อาจมีการคิดค่าบริการการใช้ API

Open API[3] เป็น API ที่หน่วยงานเปิดให้ผู้ใช้ทั่วไปสามารถเข้าถึง และใช้งานได้โดยอิสระ และไม่มีค่าใช้จ่าย

Partner API เป็น API ที่เปิดให้เฉพาะผู้ใช้จากหน่วยงานพันธมิตร หรือเฉพาะบางหน่วยงานเข้าใช้งานได้

Private API หรือ Internal API เป็น API ที่เปิดให้ใช้งานเฉพาะภายในหน่วยงานเท่านั้น

Composite API เป็นการรวมหลาย API มาไว้ในการเรียกใช้ API เพียงครั้งเดียวทำให้แอปพลิเคชันสามารถเรียกใช้งานได้อย่างมีประสิทธิภาพ และลดจำนวนการเรียกใช้ API แยก โดยหากแบ่งประเภท API ตามข้อกำหนด หรือรูปแบบโปรโตคอล สามารถแบ่งได้เป็น

- Simple Object Access Protocol (SOAP) ซึ่งมีการกำหนดข้อความในรูปแบบ XML ช่วยให้แอปพลิเคชันที่พัฒนาด้วยภาษา และสำหรับสภาพแวดล้อมที่ต่างกันสามารถแลกเปลี่ยนข้อมูลได้ ผ่านโพรโทคอล เช่น SMTP และ HTTP
- Representational State Transfer (REST) เป็นเซ็ทของหลักการสถาปัตยกรรม API สำหรับเว็บ มีการใช้โพรโทคอล HTTP ในการรับส่งข้อมูล มีฟังก์ชันพื้นฐาน ได้แก่ GET, POST, PUT, และ DELETE
- XML-RPC โพรโทคอลแบบ XML-RPC เป็นโพรโทคอลสำหรับการทำ Remote Procedure Call ระหว่างระบบทางไกลผ่านโพรโทคอล HTTP และใช้ข้อมูลในรูปแบบ XML
- JSON-RPC โพรโทรคอลแบบ JSON-RPC คล้ายกับ XML-RPC แต่มีการแลกเปลี่ยนข้อมูลในรูปแบบ JSON แทน

ถึงแม้ว่า API จะมีประโยชน์มากมาย เช่น ช่วยให้นักพัฒนาระบบสามารถพัฒนาแอปพลิเคชันได้สะดวกขึ้นโดยสามารถใช้ข้อมูล และบริการที่มีอยู่แล้วผ่าน API สามารถแบ่งปันข้อมูล และบริการให้หน่วยงานภายใน และภายนอกได้สะดวก และสามารถพัฒนาระบบแลกเปลี่ยนข้อมูลอัตโนมัติได้ แต่ API ทำให้เกิด

[3] Open API ในที่นี้ แตกต่างจาก OpenAPI Specification ซึ่งเป็นข้อกำหนดโดย Swagger https://swagger.io/specification/

ต้นทุนเพิ่มเติมทั้งในการพัฒนา และการบำรุงรักษา อีกทั้งยังจำเป็นต้องรักษาความมั่นคงปลอดภัยอย่างเหมาะสมเพื่อลดความเสี่ยงจากการเข้าถึงข้อมูล และบริการโดยไม่ได้รับอนุญาต

9.2.1. ความเสี่ยงความมั่นคงปลอดภัยที่พบบ่อย

API เป็นการเปิดให้ระบบอื่น ๆ สามารถเข้าถึงข้อมูล และบริการได้ หากมีการรักษาความมั่นคงปลอดภัยที่ไม่เหมาะสม อาจทำให้ผู้ไม่ประสงค์ดีเข้าถึงข้อมูล และบริการโดยไม่ได้รับอนุญาต และทำความเสียหายให้กับข้อมูล และระบบได้

มูลนิธิที่ไม่แสวงหาผลกำไร Open Worldwide Application Security Project (OWASP) ได้มีการจัดลำดับความเสี่ยงความมั่นคงปลอดภัยที่พบบ่อย API Security Top 10 2023 ดังนี้

API1:2023 - Broken Object Level Authorization ผู้ไม่ประสงค์ดีใช้ช่องโหว่การตรวจสอบ และให้สิทธิในการเข้าถึง Object ด้วยการระบุ Identifier

API2:2023 - Broken Authentication การนำระบบการพิสูจน์ตัวจริงไปใช้แบบไม่ถูกต้อง ทำให้ผู้ไม่ประสงค์ดีสามารถปลอมตัวเป็นผู้มีสิทธิใช้งานระบบเข้าระบบได้

API3:2023 - Broken Object Property Level Authorization ผู้ไม่ประสงค์ดีใช้ช่องโหว่การตรวจสอบ และให้สิทธิในการเข้าถึง Property ของ Object เกินสิทธิที่ควรจะเข้าถึงได้

API4:2023 - Unrestricted Resource Consumption ไม่มีการตรวจสอบ และควบคุมการใช้งานที่เหมาะสม ทำให้ผู้ไม่ประสงค์ดีอาจร้องขอบริการซึ่งต้องใช้ทรัพยากรมากเกินไป ทำให้ไม่สามารถให้บริการกับผู้อื่นได้

API5:2023 - Broken Function Level Authorization การตรวจสอบ และให้สิทธิในการเข้าใช้ฟังก์ชันไม่เหมาะสม หรือผิดพลาด ทำให้ผู้ไม่ประสงค์ดีเข้าถึงทรัพยากร หรือฟังก์ชันของผู้ใช้งานอื่น ๆ ได้

API6:2023 - Unrestricted Access to Sensitive Business Flows ผู้ไม่ประสงค์ดีค้นหา API endpoint ที่ใช้ภายในหน่วยธุรกิจ และใช้วิธีการอัตโนมัติในการเรียกใช้ API ทำให้เกิดผลกระทบเชิงลบต่อธุรกิจได้

API7:2023 – Server-Side Request Forgery เกิดขึ้นเมื่อ API เรียกใช้ทรัพยากรทางไกลโดยไม่ตรวจสอบ URL ที่ได้จากผู้ใช้งาน ทำให้ผู้ไม่ประสงค์ดีบังคับให้แอปพลิเคชันส่งคำร้องที่ปรับแต่งมาเฉพาะไปยังปลายทาง เป็นการปลอมแปลงเพื่อให้ได้ข้อมูล หรือบริการที่ไม่ควรได้

API8:2023 - Security Misconfiguration การตั้งค่าความมั่นคงปลอดภัยที่ผิดพลาดอาจเปิดช่องให้ผู้ไม่ประสงค์ดีเข้าถึงข้อมูล และระบบ ทำให้เกิดความเสียหายต่อข้อมูล และระบบได้

API9:2023 - Improper Inventory Management การบริหารจัดการรายการทรัพย์สินที่ไม่เหมาะสมทำให้ผู้ไม่ประสงค์ดีอาจเข้าถึง API เก่าที่ไม่ใช้แล้วแต่ยังไม่ได้ปิด หรือนำออกจากระบบเพื่อเข้าถึงข้อมูล หรือระบบโดยไม่ได้รับอนุญาต

API10:2023 - Unsafe Consumption of APIs เนื่องจากนักพัฒนาระบบมักจะเชื่อมั่นในผลลัพธ์ที่ได้จาก API มากกว่าข้อมูลที่นำเข้าจากผู้ใช้ ทำให้มักจะมีการควบคุมความมั่นคงปลอดภัยที่อ่อนกว่า ดังนั้นผู้ไม่ประสงค์ดีอาจจะไปเจาะระบบ API จากผู้ให้บริการภายนอกที่ให้บริการกับ API เป้าหมาย แทนการเจาะระบบไปที่ API เป้าหมายโดยตรง

รายละเอียดความเสี่ยงเพิ่มเติม และวิธีการรับมือความเสี่ยงเหล่านี้ สามารถศึกษาได้จากเว็บ OWASP API Security Top 10 2023

9.2.2. แนวทางปฏิบัติที่ดีเพื่อรักษาความมั่นคงปลอดภัย

เป้าหมายหลักของการรักษาความมั่นคงปลอดภัย API คือการวางกลยุทธ์ และมาตรการในการทำความเข้าใจ บรรเทาช่องโหว่ความมั่นคงปลอดภัย และลดความเสี่ยงจากภัยคุกคามที่มีต่อ API โดยมีการใช้วิธีการที่หลากหลายร่วมกัน เช่น การพิสูจน์ตัวจริง การให้สิทธิ การตรวจสอบ การทำความสะอาดข้อมูล และการเตรียมความพร้อมความต่อเนื่องในการให้บริการ

แนวทางปฏิบัติที่ดีเบื้องต้นเพื่อการรักษาความมั่นคงปลอดภัยมีดังต่อไปนี้

1) จัดทำรายการ และบริหารจัดการ API (API inventory and management) แต่ละหน่วยงานอาจมีการใช้งาน API จำนวนมาก หนึ่งในขั้นตอนแรกที่หน่วยงานควรทำคือการจัดทำรายการ API เพื่อให้ทราบว่ามี API ใดเปิดใช้งานอยู่บ้างเพื่อที่จะสามารถควบคุม และใช้มาตรการในการปกป้องความมั่นคงปลอดภัยได้อย่างเหมาะสม และ API ใดที่ไม่ใช้แล้วก็ควรปิด และนำออกจากระบบให้บริการ

2) ประเมินความเสี่ยงของ API ควรมีการประเมินความเสี่ยงของ API ที่เปิดใช้งานอยู่ทั้งหมดเพื่อวางแผน และจัดเตรียมมาตรการการควบคุมความมั่นคงปลอดภัยที่เหมาะสมกับแต่ละ API ควรระบุระบบ และข้อมูลที่จะได้รับผลกระทบหาก API เกิดความเสียหาย และวางแผนการควบคุม และการรับมือเพื่อลดความเสี่ยงให้อยู่ในระดับที่รับได้ ควรมีการประเมินความเสี่ยงอย่างสม่ำเสมอ โดยเฉพาะเมื่อ API มีการเปลี่ยนแปลง หรือมีภัยคุกคามที่เกิดขึ้นใหม่

3) การพิสูจน์ตัวจริง (Authentication) และการให้สิทธิ (Authorization) ที่แข็งแกร่ง ใช้โปรโตคอลการพิสูจน์ตัวจริง และการให้สิทธิมาตรฐานที่เป็นที่ยอมรับ และมีความมั่นคงปลอดภัย เช่น OAuth 2.0, API keys, JWT, และ OpenID Connect เพื่อให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตสามารถใช้งานได้ และมีการควบคุมการเข้าถึงทรัพยากรอย่างเหมาะสม เพื่อให้ผู้ใช้งานเข้าถึงได้เฉพาะทรัพยากรที่มีสิทธิเข้าถึงเท่านั้น

4) มีการบริหารจัดการข้อมูลที่ใช้ในการพิสูจน์ตัวจริงอย่างเหมาะสม ไม่ควรเก็บข้อมูลที่ใช้ในการพิสูจน์ตัวจริง เช่น กุญแจ API ในโค้ด หรือไฟล์ที่อยู่ในที่จัดเก็บโค้ดของ API อาจพิจารณาใช้บริการบริหารจัดการความลับ (Secret Management Service) เพื่อบริหารจัดการข้อมูลที่ใช้ในการพิสูจน์ตัวจริงอย่างมั่นคงปลอดภัย

5) ใช้หลักการสิทธิพิเศษขั้นต่ำ (The Principle of Least Privilege) ควรให้สิทธิกับผู้ใช้ในการเข้าใช้งาน API และเข้าถึงทรัพยากรต่าง ๆ ด้วยสิทธิพิเศษขั้นต่ำเท่าที่จำเป็นต่อการดำเนินงานของผู้ใช้ ควรใช้หลักการนี้กับทุก API ที่มี

6) นำข้อมูลที่ไม่ต้องการเปิดเผยออก นักพัฒนาระบบมักจะมีการเก็บข้อมูล เช่น รหัสผ่าน และกุญแจ และข้อมูลอื่น ๆ ที่อาจจะเกินความจำเป็นใน API ระหว่างการพัฒนา และทดสอบระบบเพื่อความสะดวกในการพัฒนา ควรลบข้อมูลเหล่านี้ออกจาก API ก่อนที่จะเปิด API ให้บริการกับผู้ใช้ หน่วยงานอาจใช้เครื่องมือสแกนเพื่อตรวจสอบข้อมูลที่ไม่จำเป็นต้องเปิดเผยก่อนเปิดให้ผู้ใช้ใช้งาน หรือไม่

7) ใช้โพรโทคอลที่มีการเข้ารหัสลับ (Encryption Protocol) ใช้โพรโทคอลที่มีการเข้ารหัสลับเช่น TLS หรือ HTTPS เพื่อสร้างการเชื่อมต่อที่มีความมั่นคงปลอดภัย ปกป้องจากการเข้าถึงและแก้ไขข้อมูลโดยไม่ได้รับอนุญาต นอกจากนี้ข้อมูลที่มีความละเอียดอ่อน เช่น รหัสผ่าน ควรมีการเข้ารหัสลับในระหว่างที่จัดเก็บด้วย

8) พิจารณาใช้ Web Application Firewall (WAF) WAF เพิ่มการปกป้องความมั่นคงปลอดภัยอีกชั้นหนึ่งให้กับ API ของหน่วยงาน โดยเฉพาะจากการโจมตีที่พบได้บ่อย เช่น Injection attack, Cross-Site Scripting (XSS), และ Cross-Site Request Forgery (CSRF) WAF ช่วยวิเคราะห์และบล็อก traffic ที่ไม่ประสงค์ดีก่อนจะถูกส่งไปยังเซิร์ฟเวอร์

9) พิจารณาใช้งาน API Gateway การใช้ API Gateway เป็นการสร้างทางเข้าทางเดียวสำหรับทุกคำขอใช้ API และเป็นชั้นที่เพิ่มการควบคุมความมั่นคงปลอดภัยต่าง ๆ ได้ นอกจากนี้ยังสามารถเพิ่มคุณสมบัติอื่น ๆ เช่น request / response transformation, caching, และ logging

10) การตรวจสอบข้อมูล (Data Validation) มีการตรวจสอบข้อมูลที่รับเข้ามาที่ API ก่อนที่จะมีการประมวลผล ตรวจสอบว่าข้อมูลมาในรูปแบบที่ถูกต้อง หรือไม่ มีขนาดเหมาะสม หรือไม่ มีลักษณะที่ผิดแปลกไปจากข้อมูลที่ควรจะเป็น หรือไม่ เป็นต้น สามารถใช้ XML หรือ JSON schema validation ช่วยตรวจสอบตัวแปร หรือพารามิเตอร์ต่าง ๆ ได้

11) การควบคุมปริมาณการใช้งาน (Rate Limiting) มีการจำกัดปริมาณคำขอที่ส่งมายัง API จากผู้ใช้งาน หรือ IP ในช่วงระยะเวลาหนึ่งเพื่อปกป้องทรัพยากรจากการโจมตีแบบ Brute Force และ DoS การควบคุมปริมาณยังช่วยให้ระบบสามารถประมวลผลคำขอจากแต่ละผู้ใช้งานได้อย่างมีประสิทธิภาพ ไม่มีผู้ใช้งานคนใดคนหนึ่งเอาเปรียบ หรือส่งคำขอจนทำให้ระบบไม่สามารถให้บริการผู้ใช้อื่นได้

12) การทดสอบความมั่นคงปลอดภัย (Security Testing) มีการส่งคำร้องขอไปยัง API เพื่อตรวจสอบความถูกต้อง และคุณภาพของผลลัพธ์ที่ส่งกลับจาก API การทดสอบด้านความมั่นคงปลอดภัยต่าง ๆ เช่น Penetration Test, Injection Test, Authentication Test, Parameter Tampering, และอื่น ๆ เป็นประจำจะช่วยให้นักพัฒนาระบบสามารถพบช่องโหว่ความมั่นคงปลอดภัย และสามารถแก้ไขปัญหาได้ก่อนที่ผู้ไม่ประสงค์ดีจะใช้ประโยชน์จากช่องโหว่ในการโจมตีระบบ

13) การเฝ้าระวัง และการแพทช์ API (API Monitoring and Patching) เฝ้าระวังและสังเกตว่ามีกิจกรรมเครือข่ายที่ผิดปกติ หรือไม่ ปรับปรุง API ด้วยแพทช์ความมั่นคงปลอดภัยล่าสุดอยู่

เสมอ นอกจากนี้นักพัฒนาระบบ หรือผู้ดูแลระบบควรตระหนักถึงภัยคุกคามที่พบบ่อย เช่น OWASP API Security Top 10 และเตรียมพร้อมกับการรับมือภัยคุกคามเหล่านี้

14) การตรวจสอบ และการเก็บล็อก (Auditing and Logging) เก็บข้อมูลที่สำคัญลงล็อก และมีการทบทวนล็อกเป็นประจำ และสม่ำเสมอเพื่อติดตาม และตรวจสอบการใช้งานระบบของผู้ใช้ว่ามีการเข้าถึงระบบใดบ้าง การตรวจสอบเป็นประจำจะช่วยให้ประหยัดเวลาในการตรวจสอบเมื่อเกิดเหตุการณ์ที่ไม่คาดคิด หรือเกิดปัญหาอื่น ๆ นอกจากนี้ข้อมูลส่วนใหญ่ในล็อกมักจะเป็นกิจกรรมปกติซึ่งสามารถใช้เป็นการประเมินพื้นฐาน (Baseline) ในการตรวจพบกิจกรรมที่ไม่ปกติได้

15) การเก็บรายการเวอร์ชัน และการเตรียมเอกสารประกอบ (Versioning and Documentation) API เวอร์ชันใหม่จะมีการปรับปรุง และแพทช์ความมั่นคงปลอดภัยเพื่อแก้ไขปัญหาต่าง ๆ ของ API เวอร์ชันก่อนหน้า หากไม่มีการเก็บรายการเวอร์ชัน และเตรียมเอกสารประกอบที่ดี อาจมีผู้ที่นำ API เวอร์ชันเก่าที่มีปัญหาความมั่นคงปลอดภัยไปติดตั้ง และใช้งานระบบทำให้เกิดความเสี่ยงได้ เอกสารประกอบควรมีความชัดเจน ครบถ้วน มีการระบุตัวแปร และรูปแบบข้อมูลนำเข้าที่ชัดเจน ผลลัพธ์ที่ควรจะเป็น และข้อกำหนดด้านความมั่นคงปลอดภัย

สำหรับผู้ที่สนใจรายละเอียดเกี่ยวกับแนวปฏิบัติที่ดีในการใช้งาน API อย่างมีความมั่นคงปลอดภัย สามารถศึกษาข้อมูลเพิ่มเติมได้จากแหล่งข้อมูล และเอกสารดังต่อไปนี้

- API Security Top 10 2023, OWASP, https://owasp.org/www-project-api-security/
- Security Guidelines for Providing and Consuming APIs, CSA, https://cloudsecurityalliance.org/artifacts/security-guidelines-for-providing-and-consuming-apis
- Securing APIs: 10 Best Practices for Keeping Your Data and Infrastructure Safe, F5, https://www.f5.com/labs/learning-center/securing-apis-10-best-practices-for-keeping-your-data-and-infrastructure-safe
- Optimize APIs with API security best practices, IBM, https://www.ibm.com/blog/api-security-best-practices/

9.3. แนวปฏิบัติการพัฒนาโปรแกรมอย่างมั่นคงปลอดภัย (Secure Coding Guideline)

การพัฒนาโปรแกรม หรือการพัฒนาแอปพลิเคชัน หมายถึง การพัฒนาชุดคำสั่ง หรือโปรแกรม เพื่อให้คอมพิวเตอร์สามารถทำงานตามที่ได้รับมอบหมายได้ ในบางที่อาจจะมีการแยก Programming และ Coding โดย Programming หมายถึงกระบวนการต่าง ๆ ที่เกี่ยวข้องตลอดช่วงเวลาการพัฒนาโปรแกรม เช่น วางแผน ออกแบบ เลือกโครงสร้างข้อมูล และอัลกอริทึมที่จะใช้ในการพัฒนาโปรแกรม และการทดสอบโปรแกรม รวมถึงการบริหารจัดการโครงการ ส่วน Coding หมายถึงกระบวนการเขียนชุดคำสั่งให้คอมพิวเตอร์ดำเนินการตามฟังก์ชันของโปรแกรมที่ได้ออกแบบ และวางแผนไว้ โดยทั่วไปนักพัฒนาโปรแกรมใช้ภาษาการเขียนระดับสูง (High-level Programming Language) ในการเขียนโปรแกรม ไม่นิยมใช้รหัสเครื่อง (Machine Code) ในการเขียนโปรแกรมโดยตรง

โปรแกรมต่าง ๆ โดยทั่วไปมักจะมีจุดอ่อน ส่วนที่ทำให้เกิดความผิดพลาดในการทำงาน หรือช่องโหว่ความมั่นคงปลอดภัยที่อาจถูกค้นพบ และใช้ประโยชน์โดยผู้ไม่ประสงค์ดีเพื่อเข้าถึงระบบ และข้อมูลที่มีความสำคัญ และละเอียดอ่อนได้ นักพัฒนาโปรแกรมจึงควรมีความเข้าใจกับจุดอ่อนของโปรแกรมที่พบได้บ่อย และรู้จักการพัฒนาโปรแกรมอย่างมั่นคงปลอดภัยเพื่อให้โปรแกรมสามารถทำงานได้ตรงตามวัตถุประสงค์ และลดความเสี่ยงจากการถูกผู้ไม่ประสงค์ดีใช้ประโยชน์จากช่องโหว่ความมั่นคงปลอดภัย

9.3.1. ช่องโหว่ความมั่นคงปลอดภัยที่พบบ่อย

รายการ Common Weakness Enumeration (CWE)[4] เป็นรายการที่รวบรวมประเภทจุดอ่อนของซอฟท์แวร์ และฮาร์ดแวร์ที่พัฒนาโดยกลุ่มชุมชนเพื่อใช้เป็นภาษากลางในการสื่อสาร ไม้วัดสำหรับเครื่องมือความมั่นคงปลอดภัย และการประเมินพื้นฐาน (Baseline) ในการระบุ การบรรเทา และการป้องกันของจุดอ่อน

สำนักงานความมั่นคงปลอดภัยไซเบอร์ และโครงสร้างพื้นฐาน (Cybersecurity and Infrastructure Security Agency [CISA]) สหรัฐอเมริการได้จัดทำรายการประเภทช่องโหว่ที่ถูกใช้ประโยชน์บ่อย (Known Exploited Vulnerabilities [KEV] Catalog) ประจำปี พ.ศ. 2566 ซึ่งมีรายการช่องโหว่ดังต่อไปนี้[5]

1) **Use After Free (CWE-416)** มีการอ้างอิงถึงหน่วยความจำที่ได้มีการคืนการใช้งานแล้ว อาจทำให้โปรแกรมไม่สามารถทำงานได้ ใช้ค่าที่ไม่ถูกต้อง หรือรันโค้ดที่ไม่พึงประสงค์

2) **Heap-Based Buffer Overflow (CWE-122)** บัฟเฟอร์เก็บข้อมูลที่เป็นฮีปอาจล้นและมีการเขียนข้อมูลทับไปในหน่วยความจำเกินที่จองไว้ อาจทำให้เกิดปัญหาต่าง ๆ ได้ เช่น โปรแกรมไม่สามารถทำงานได้ หรือรันโค้ดไม่พึงประสงค์

[4] https://cwe.mitre.org/

[5] https://cwe.mitre.org/top25/archive/2023/2023_kev_list.html

3) Out-of-Bounds Write (CWE-787) มีการเขียนข้อมูลเกินขนาดของบัฟเฟอร์ที่จองไว้ที่ก่อนจุดเริ่มต้น หรือจุดสิ้นสุดของบัฟเฟอร์ อาจทำให้โปรแกรมทำงานผิดพลาด รันโค้ดไม่พึงประสงค์ หรือข้อมูลผิดพลาด

4) Improper Input Validation (CWE-20) โปรแกรมมีการรับข้อมูลเข้า (เช่น จากผู้ใช้งาน) แต่ไม่มีการตรวจสอบข้อมูลอย่างเหมาะสม โปรแกรมที่นำข้อมูลไปใช้อาจทำงานผิดพลาด หรือรันคำสั่งอันตรายที่อยู่ในข้อมูลได้

5) Improper neutralization of special elements used in an OS command ('OS command injection') (CWE-78) โปรแกรมมีการใช้คำสั่งของระบบปฏิบัติการ และมีการใช้ค่าบางอย่างจากข้อมูลที่นำเข้า แต่ไม่มีการตรวจสอบข้อมูลนำเข้าที่เหมาะสม อาจทำให้คำสั่งระบบปฏิบัติการทำงานเกินขอบเขตที่กำหนด

6) Deserialization of Untrusted Data (CWE-502) โปรแกรมมีการแปลงข้อมูลที่ไม่น่าเชื่อถือกลับมาโดยไม่มีการตรวจสอบว่าผลลัพธ์อยู่ในรูปแบบที่ปลอดภัยต่อการใช้งาน หรือไม่

7) Server-Side Request Forgery (SSRF) (CWE-918) เซิร์ฟเวอร์ได้รับคำร้องขอเข้าถึง URL จากผู้ไม่ประสงค์ดีและเข้าถึง URL โดยไม่ได้ตรวจสอบว่าเป็นปลายทางที่สมควรเข้าถึงหรือไม่

8) Access of Resource using Incompatible Type ('Type Confusion') (CWE-843) โปรแกรมจัดสรรทรัพยากร เช่น pointer, object, หรือ variable ที่เป็นประเภทหนึ่ง แต่ภายหลังมีการเข้าถึงทรัพยากรนั้นด้วยประเภทที่ไม่เข้ากันกับประเภทดั้งเดิมที่ได้ประกาศไว้

9) Improper limitation of a pathname to a restricted directory ('Path Traversal') (CWE-22) โปรแกรมมีการนำเข้าข้อมูล pathname จากภายนอกที่ชี้ไปยังทรัพยากรที่ถูกจำกัดการเข้าถึงโดยไม่ได้ตรวจสอบ pathname และจำกัดการเข้าถึงอย่างเหมาะสม

10) Missing Authentication for Critical Function (CWE-306) โปรแกรมไม่มีการทำการพิสูจน์ตัวจริงก่อนเข้าถึงฟังก์ชันสำคัญที่ต้องตรวจสอบอัตลักษณ์ผู้ใช้หรือฟังก์ชันที่มีการใช้ทรัพยากรจำนวนมาก

รายละเอียดเพิ่มเติม และข้อมูลประเภทช่องโหว่ที่พบได้บ่อยอื่น ๆ สามารถศึกษาได้จากเว็บไซต์ CWE

9.3.2. แนวทางปฏิบัติที่ดีเพื่อรักษาความมั่นคงปลอดภัย

การรักษาความมั่นคงปลอดภัยสารสนเทศไม่ใช่เพียงการเพิ่มมาตรการควบคุมความมั่นคงปลอดภัยให้กับระบบต่าง ๆ หลังจากที่ระบบนั้นได้ติดตั้งใช้งานในสภาพแวดล้อมจริงเท่านั้น แต่การรักษาความมั่นคงปลอดภัยที่ดีควรเริ่มตั้งแต่การออกแบบ และพัฒนาระบบให้มีความมั่นคงปลอดภัย การพัฒนาโปรแกรมอย่างมั่นคงปลอดภัยคือการใช้แนวปฏิบัติที่ดีในการออกแบบ และพัฒนาโปรแกรมเพื่อปกป้องโปรแกรมจากช่องโหว่ความมั่นคงปลอดภัยที่เป็นที่รู้จักแล้ว ที่ยังไม่เป็นที่รู้จัก และที่ไม่คาดคิด เช่น การใช้ข้อผิดพลาดทางตรรกะของโปรแกรม และการสูญหายของข้อมูลที่ใช้ในการพิสูจน์ตัวจริง ช่องโหว่ความมั่นคงปลอดภัยจำนวน

มากเกิดจากข้อผิดพลาดในการพัฒนาโปรแกรมที่พบได้บ่อย ดังนั้นการพัฒนาโปรแกรมอย่างมีความมั่นคงปลอดภัยจึงสามารถช่วยลดปัญหาช่องโหว่ความมั่นคงปลอดภัยได้ก่อนที่มีการนำโปรแกรมไปติดตั้งใช้งานจริง โดยทั่วไปแล้วต้นทุนในการพัฒนาโปรแกรมให้มีความมั่นคงปลอดภัยตั้งแต่เริ่มต้นมักจะถูกกว่าต้นทุนในการแก้ไขปัญหาความมั่นคงปลอดภัยหลังจากที่ได้กระจายโปรแกรมไปแล้วซึ่งยังไม่รวมถึงค่าใช้จ่ายที่อาจเกิดขึ้นถ้าช่องโหว่ความมั่นคงปลอดภัยดังกล่าวถูกนำไปใช้ทำให้เกิดความเสียหาย

เอกสารฉบับนี้นำเสนอแนวปฏิบัติที่ดีเบื้องต้นในการพัฒนาโปรแกรมอย่างมั่นคงปลอดภัย อ้างอิงจาก Secure coding practices โดย มูลนิธิที่ไม่แสวงหาผลกำไร Open Worldwide Application Security Project (OWASP)[6] แนวปฏิบัตินี้สามารถใช้ได้กับการพัฒนาโปรแกรมโดยทั่วไป ไม่จำกัดเฉพาะการพัฒนาเว็บแอปพลิเคชันเท่านั้น โดยแนวปฏิบัติหลักมีดังต่อไปนี้

1) การตรวจสอบข้อมูลนำเข้า (Input Validation) มีการตรวจสอบข้อมูลทั้งหมด โดยเฉพาะข้อมูลที่มาจากแหล่งที่ไม่น่าเชื่อถือ การตรวจสอบข้อมูลควรทำบนระบบที่เชื่อถือได้ (ที่ฝั่งเซิร์ฟเวอร์ ไม่ใช่เพียงฝั่งไคลเอนท์) มีการกำหนดชุดรหัสอักษร (Character Set) เช่น UTF-8 อนุญาตเฉพาะประเภทข้อมูลที่ระบบรองรับ ตรวจสอบขนาด และความยาวของข้อมูล ไม่นำข้อมูลที่ไม่ผ่านการตรวจสอบมาทำการประมวลผลต่อ หากจำเป็นจะต้องประมวลผลข้อมูลที่อาจมีความเสี่ยง ควรเตรียมการควบคุมเพิ่มเติมเพื่อเสริมการปกป้อง

2) การเข้ารหัสผลลัพธ์ (Output Encoding) มีการเข้ารหัสผลลัพธ์บนระบบที่เชื่อถือได้ (ที่ฝั่งเซิร์ฟเวอร์) มีการใช้การเข้าหัสที่เป็นมาตรฐาน และผ่านการทดสอบ มีการกำหนดชุดรหัสอักษร ตรวจสอบว่าการเข้ารหัสผลลัพธ์สามารถใช้งาน และปลอดภัยต่อระบบเป้าหมายที่รองรับ มีการทำความสะอาดข้อมูลที่มาจากแหล่งไม่น่าเชื่อถือ มีการตรวจสอบ และทำความสะอาดข้อมูลที่จะส่งต่อไปยังคำสั่งระบบปฏิบัติการ

3) การพิสูจน์ตัวจริง และการบริหารจัดการรหัสผ่าน (Authentication and Password Management) มีการพิสูจน์ตัวจริงก่อนเข้าถึงทรัพยากรทุกอย่าง ยกเว้นทรัพยากรที่เปิดให้เข้าถึงโดยสาธารณะ การควบคุมการพิสูจน์ตัวจริงจะต้องทำบนระบบที่เชื่อถือได้ ใช้การพิสูจน์ตัวจริงที่มีมาตรฐานเป็นที่ยอมรับ และผ่านการทดสอบ การควบคุมการพิสูจน์ตัวจริงหากเกิดข้อผิดพลาดจะต้องปิดการทำงานได้อย่างปลอดภัย ฟังก์ชันการบริหาร และการจัดการบัญชีอย่างน้อยจะต้องมั่นคงปลอดภัยระดับเดียวกับกลไกการพิสูจน์ตัวจริงหลัก หากมีการเก็บรหัสผ่านเองควรใช้ฟังก์ชัน Hash และ Salt ที่มีความมั่นคงปลอดภัย ผลลัพธ์การพิสูจน์ตัวจริงที่ไม่ผ่านไม่ควรเปิดเผยว่าข้อมูลส่วนใดไม่ถูกต้อง การเก็บ Credential ในการพิสูจน์ตัวจริงควรเก็บในที่ที่ปลอดภัย รหัสผ่านควรมีการเข้ารหัสลับก่อนส่งข้อมูลผ่านเครือข่าย หากมีการใส่รหัสผ่านผิดเป็นจำนวนหนึ่งควรมีการปิดการเข้าล็อกอินไปช่วงเวลาหนึ่งเพื่อเพิ่มความยากในการทำ Brute Force Attack การตั้งรหัสผ่านใหม่ หรือการลืมรหัสผ่านจะต้องมีความมั่นคงปลอดภัยเท่ากับการสร้างบัญชี และการพิสูจน์ตัวจริง หากมีการใช้รหัสผ่าน หรือลิงค์ชั่วคราวในการพิสูจน์ตัวจริง ควรกำหนดอายุให้สั้น

[6]https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/

เพียงพอ เปลี่ยนรหัสผ่านดั้งเดิมที่มากับผลิตภัณฑ์ที่ใช้ ทำการพิสูจน์ตัวจริงผู้ใช้งานซ้ำก่อนจะเรียกใช้ฟังก์ชันที่มีความสำคัญสูง และการเข้าถึงทรัพยากรที่สำคัญ และมีความละเอียดอ่อนควรพิจารณาใช้การพิสูจน์ตัวจริงหลายปัจจัย

4) การบริหารจัดการเซสชั่น (Session Management) มีการใช้งานการควบคุมการบริหารจัดการเซสชันของเซิร์ฟเวอร์ หรือเฟรมเวิร์กที่ใช้ การสร้าง Session Identifier ควรทำบนระบบที่เชื่อถือได้ การควบคุมการบริหารจัดการเซสชั่นควรใช้อัลกอริทึมที่สุ่ม Session Identifier ที่มีความสุ่มเพียงพอ ฟังก์ชันการล็อกเอาท์จะต้องยุติการเชื่อมต่อ และเซสชั่นอย่างเหมาะสม และควรมีฟังก์ชันล็อกเอาท์ทุกหน้าที่มีการให้สิทธิเข้าถึงทรัพยากร มีการตั้งเวลา Session Timeout อย่างเหมาะสมโดยคำนึงถึงความเสี่ยง และการทำธุรกิจ มีการสร้าง Session Identifier ใหม่ทุกครั้งเมื่อมีการพิสูจน์ตัวจริงใหม่

5) การควบคุมการเข้าถึง (Access Control) การตัดสินใจอนุญาตให้สิทธิควรทำโดยระบบที่เชื่อถือได้เท่านั้น การควบคุมการเข้าถึงหากเกิดข้อผิดพลาดจะต้องปิดการทำงานได้อย่างปลอดภัย ปฏิเสธการเข้าถึงทุกคำร้องขอถ้าโปรแกรมไม่สามารถเข้าถึงข้อมูลการตั้งค่าความมั่นคงปลอดภัยได้ บังคับใช้การควบคุมการเข้าถึงทุกคำร้องขอรวมถึงสคริปต์จากฝั่งเซิร์ฟเวอร์ แยกตรรกะสิทธิพิเศษออกจากโค้ดโปรแกรมอื่น ๆ จำกัดการเข้าถึงทรัพยากรให้เฉพาะผู้ที่ได้รับอนุญาต และมีสิทธิในการเข้าถึงเท่านั้น ถ้าต้องมีการเก็บข้อมูลสถานะที่ฝั่งไคลเอนท์ ควรใช้การเข้ารหัสลับ และการตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลด้วย ถ้ามีการใช้เซสชันเป็นระยะเวลานาน ควรมีการตรวจสอบการให้สิทธิเข้าถึงกับผู้ใช้เป็นระยะเพื่อตรวจสอบว่าสิทธิของผู้ใช้ยังไม่เปลี่ยนแปลง หากมีการเปลี่ยนแปลง ให้ล็อกเอาท์ผู้ใช้จากระบบ และทำการล็อกอินใหม่ มีการตรวจสอบบัญชี และปิดใช้งานบัญชีที่ไม่มีการใช้งาน โปรแกรมควรรองรับการปิดบัญชีและตัดการเชื่อมต่อเมื่อการให้สิทธิสิ้นสุดลง บัญชีสำหรับการบำรุงรักษา หรือบัญชีที่เชื่อมต่อกับภายนอกควรให้สิทธิพิเศษน้อยที่สุดที่เป็นไปได้ที่เพียงพอต่อการปฏิบัติงาน

6) การใช้งานระบบรหัสลับ (Cryptographic Practices) ฟังก์ชันระบบรหัสลับที่ปกป้องความลับจะต้องอยู่บนระบบที่เชื่อถือได้ ปกป้องความลับจากการเข้าถึงโดยไม่ได้รับอนุญาต โมดูลระบบรหัสลับหากเกิดข้อผิดพลาดจะต้องปิดการทำงานอย่างปลอดภัย ข้อมูลค่าสุ่มต่าง ๆ จะต้องเกิดจากหน่วยสร้างเลขสุ่ม (Random number generator) ที่โมดูลระบบรหัสลับรับรอง โมดูลระบบรหัสลับที่ใช้ควรมีมาตรฐานเป็นที่ยอมรับ และผ่านการทดสอบอย่างเหมาะสม สร้างนโยบาย และกระบวนการการบริหารจัดการกุญแจรหัสลับ

7) การจัดการ และการเก็บบันทึกข้อผิดพลาด (Error Handling and Logging) ไม่เปิดเผยข้อมูลละเอียดอ่อนในการตอบสนองข้อผิดพลาด รวมถึง รายละเอียดระบบ Session Identifier และ ข้อมูลบัญชี ใช้ตัวจัดการข้อผิดพลาดที่ไม่แสดงข้อมูล Debugging และ Stack Trace มีการใช้ข้อความข้อผิดพลาดทั่วไป (Generic Error Message) และหน้าข้อผิดพลาดเฉพาะ (Custom Error Page) โปรแกรมควรจัดการข้อผิดพลาดของโปรแกรมด้วยตัวเอง ไม่พึ่งพาการตั้งค่าของเครื่องเซิร์ฟเวอร์ มีการปล่อยคืนหน่วยความจำที่ได้รับจัดสรรเมื่อเกิดข้อผิดพลาดในการทำงาน ตรรกะในการจัดการข้อผิดพลาดที่เกี่ยวกับการควบคุมความมั่นคงปลอดภัยควรตั้งค่าเริ่มต้นเป็นปฏิเสธการเข้าถึง การควบคุมการเก็บบันทึกข้อผิดพลาดควร

ทำบนระบบที่เชื่อถือได้ ไม่ให้ข้อมูลที่ไม่น่าเชื่อถือที่เก็บในล็อกสามารถถูกรันเป็นโค้ดในซอฟท์แวร์ที่ใช้ในการอ่านล็อก จำกัดการเข้าถึงล็อกให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาต ไม่เก็บข้อมูลละเอียดอ่อนไว้ในล็อก เช่น รหัสผ่าน หรือ Session Identifier เก็บข้อมูลเหตุการณ์ที่สำคัญต่อความมั่นคงปลอดภัย เช่น การพิสูจน์ตัวจริง การให้สิทธิ การตรวจสอบข้อมูลนำเข้าที่ไม่ผ่าน การเปลี่ยนแปลงสถานะของข้อมูลสำคัญ ข้อผิดพลาดที่เกิดขึ้นของระบบ การใช้งานฟังก์ชันด้วยสิทธิผู้ดูแลระบบ ข้อผิดพลาดของโมดูลระบบรหัสลับ มีมาตรการในการตรวจสอบความครบถ้วนสมบูรณ์ของล็อก

8) การปกป้องข้อมูล (Data Protection) ใช้หลักการสิทธิพิเศษขั้นต่ำ ให้สิทธิเท่าที่จำเป็นกับผู้ใช้งานในการเข้าถึงทรัพยากรที่จำเป็นต่อการปฏิบัติงานเท่านั้น ปกป้องข้อมูลสำเนาชั่วคราว และ Cache ของข้อมูลละเอียดอ่อนไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าถึง และลบข้อมูลเหล่านี้เมื่อไม่มีการใช้งานแล้ว มีการเข้ารหัสลับเพื่อปกป้องความลับของข้อมูลละเอียดอ่อน และข้อมูลสำคัญ ปกป้องโค้ดของเซิร์ฟเวอร์ไม่ให้ถูกดาวน์โหลดโดยผู้ใช้ทั่วไป ลบข้อมูลที่ไม่จำเป็นต่อการทำงานที่อาจเปิดเผยข้อมูลสำคัญของระบบจากโค้ดบนระบบที่ใช้งานจริงที่ผู้ใช้เข้าถึงได้ ปิดความสามารถ Auto Complete บนฟอร์มที่จะต้องมีการใส่ข้อมูลละเอียดอ่อน เช่น บัญชีผู้ใช้ และรหัสผ่าน ปิดการเก็บ Cache บนฝั่งไคลเอนท์สำหรับหน้าที่แสดงข้อมูลละเอียดอ่อน มีการลบข้อมูลละเอียดที่ไม่มีการใช้งานอีกต่อไป มีมาตรการควบคุมการเข้าถึงข้อมูลละเอียดอ่อน

9) ความมั่นคงปลอดภัยในการสื่อสาร (Communication Security) มีการเข้ารหัสลับข้อมูลละเอียดอ่อนที่ส่งผ่านเครือข่าย เช่น การใช้การเชื่อมต่อแบบ TLS หรือการเข้ารหัสลับเฉพาะบางข้อมูล หากใช้การเชื่อมต่อแบบ TLS ใบรับรอง TLS ควรจะต้องไม่หมดอายุ และมีชื่อโดเมนที่ถูกต้อง หากการเชื่อมต่อ TLS ล้มเหลวไม่ควรลดระดับไปใช้การเชื่อมต่อที่ไม่มั่นคงปลอดภัย ใช้การตั้งค่า TLS ที่ถูกต้องเหมาะสม มั่นคงปลอดภัย มีการกำหนดชุดอักษรที่ใช้ทุกการเชื่อมต่อ มีการกรองพารามิเตอร์ที่มีข้อมูลละเอียดอ่อนจาก HTTP referrer เมื่อเชื่อมต่อไปยังภายนอก

10) การตั้งค่าระบบ (System Configuration) เวอร์ชันของเซิร์ฟเวอร์ เฟรมเวิร์ค และหน่วยของระบบจะต้องเป็นเวอร์ชันล่าสุดที่ได้รับการรับรอง และมีการติดตั้งแพทช์บำรุงรักษาความมั่นคงปลอดภัยเป็นประจำ จำกัดสิทธิของเซิร์ฟเวอร์เว็บโปรเซส และบัญชีบำรุงรักษาให้สิทธิขั้นต่ำที่สุดเท่าที่จำเป็น เมื่อเกิดข้อผิดพลาดกับระบบจะต้องปิดการทำงานลงอย่างมั่นคงปลอดภัย ปิดฟังก์ชันการใช้งานที่ไม่จำเป็น และลบข้อมูลที่ไม่จำเป็นออกจากระบบ ปิดการใช้งาน และลบออกโค้ด หรือฟังก์ชันทดสอบออกจากระบบที่มีการติดตั้งในสภาพแวดล้อมใช้งานจริง การตั้งค่าความมั่นคงปลอดภัยสามารถนำออกให้อยู่ในรูปแบบที่อ่านโดยมนุษย์ได้เพื่อการทบทวนตรวจสอบ มีระบบจัดการการเปลี่ยนแปลงซอฟท์แวร์ (Software Change Control System) เพื่อบริหารจัดการ และบันทึกการเปลี่ยนแปลงการตั้งค่า และโค้ด

11) ความมั่นคงปลอดภัยของฐานข้อมูล (Database Security) ใช้การสืบค้นข้อมูลแบบที่ใช้พารามิเตอร์ที่มีการกำหนดประเภทที่เข้มงวด มีการตรวจสอบข้อมูลนำเข้า และเข้ารหัสผลลัพธ์ หากไม่ผ่านการตรวจสอบ ไม่ควรประมวลการสืบค้นนั้น ๆ ต่อ โปรแกรมควรเข้าถึงฐานข้อมูลด้วยสิทธิพิเศษขั้นต่ำเท่าที่จำเป็น ใช้ Credential ที่มีความมั่นคงปลอดภัย ไม่ควรเก็บบันทึก Connection String ไว้ในโปรแกรม ควรเก็บแยกในไฟล์การตั้งค่าบนระบบที่เชื่อถือได้ และมีการเข้ารหัสลับ มีการจัดมุมมองฐานข้อมูลอย่าง

เหมาะสม และสามารถลบสิทธิการเข้าถึงตารางในฐานข้อมูลได้ ปิดการเชื่อมต่อเมื่อเลิกใช้งาน เปลี่ยนรหัสผ่านผู้ดูแลระบบฐานข้อมูลเริ่มต้น ปิดฟังก์ชันฐานข้อมูลที่ไม่จำเป็น ลบข้อมูลที่ไม่จำเป็น ปิดการใช้งานบัญชีที่ไม่จำเป็น โปรแกรมควรเชื่อมต่อฐานข้อมูลโดยใช้ Credential ที่เหมาะสมของแต่ละผู้ใช้งาน เช่น ผู้ใช้ที่อ่านได้อย่างเดียว Guest และผู้ดูแลระบบ

12) การบริหารจัดการไฟล์ (File Management) ไม่นำเข้าข้อมูลที่ได้จากผู้ใช้โดยตรงเข้าสู่ Dynamic Include Function มีการพิสูจน์ตัวจริงผู้ใช้ก่อนอัพโหลดไฟล์เข้าสู่ระบบ จำกัดประเภทของไฟล์ที่สามารถนำเข้าสู่ระบบได้ ตรวจสอบประเภทของไฟล์จาก File Header ไม่ใช่เพียงตรวจสอบ File Extension ป้องกัน หรือจำกัดไฟล์ที่อาจทำงานได้บนเซิร์ฟเวอร์เว็บ ปิดสิทธิการรันไฟล์บนโฟลเดอร์ที่รับไฟล์จากภายนอก เมื่ออ้างอิงถึงไฟล์ที่มีอยู่ ควรใช้รายการอนุญาต (Allow List) ชื่อไฟล์ และประเภท ไม่ส่ง Absolute File Path ไปยัง Client ทรัพยากรของโปรแกรมควรเป็นแบบอ่านเพียงอย่างเดียวเพื่อป้องกันการแก้ไข ตรวจสอบว่าไฟล์ที่ได้จากผู้ใช้มีซอฟท์แวร์ หรือโค้ดที่ไม่พึงประสงค์ หรือไม่

13) การบริหารหน่วยความจำ (Memory Management) มีการควบคุมข้อมูลนำเข้าและข้อมูลส่งออกสำหรับข้อมูลที่ไม่น่าเชื่อถือ ตรวจสอบว่าบัฟเฟอร์มีขนาดเพียงพอตามที่ระบุ หากมีการรับข้อมูลเป็นแบบ Byte ควรมีการจัดการ NULL ที่เหมาะสม มีการตรวจสอบขอบเขตของบัฟเฟอร์โดยเฉพาะในฟังก์ชันที่ทำงานวนลูป และป้องกันการ Overflow ตัดทอน (Truncate) ข้อมูลนำเข้าสตริงให้มีความยาวที่เหมาะสมก่อนส่งต่อไปยังฟังก์ชันอื่น มีการจัดการการเก็บขยะ และเก็บคืนหน่วยความจำอย่างเหมาะสม หลีกเลี่ยงการใช้งานฟังก์ชันที่มีช่องโหว่ความมั่นคงปลอดภัย เก็บคืนหน่วยความจำเมื่อจบการทำงานของฟังก์ชัน มีการลบ หรือเขียนทับข้อมูลละเอียดอ่อนที่เก็บในหน่วยความจำหลังเลิกใช้งาน

14) แนวปฏิบัติทั่วไปสำหรับการเขียนโค้ด (General Coding Practices) ใช้งานโค้ดที่เคยผ่านการทดสอบ และรับรองสำหรับงานทั่วไป ไม่ควรเขียนโค้ดใหม่ขึ้นเองทุกครั้ง เลือกใช้ API ที่มีอยู่เพื่อดำเนินการที่เกี่ยวข้องกับระบบปฏิบัติการ หลีกเลี่ยงการเรียกคำสั่งระบบปฏิบัติการโดยตรง มีกลไกและกระบวนการในการตรวจสอบความครบถ้วนสมบูรณ์ของโค้ด โปรแกรม และการตั้งค่า มีการจัดการคำร้องขอที่เกิดขึ้นพร้อม ๆ กันอย่างเหมาะสมเพื่อป้องกัน Race Condition ปกป้องทรัพยากรที่มีการใช้งานร่วมกันจากการเข้าถึงพร้อมกันที่ไม่เหมาะสม มีการตั้งค่าเริ่มต้นของตัวแปรอย่างเหมาะสมไม่ว่าจะตอนประกาศตัวแปร หรือก่อนใช้งานครั้งแรก ในกรณีที่จำเป็นต้องมีการเพิ่มระดับสิทธิในการทำงาน ควรเริ่มให้ช้าที่สุด และยุติให้เร็วที่สุดเท่าที่ทำได้ ทำความเข้าใจถึงการเก็บ และประมวลผลข้อมูลเพื่อหลีกเลี่ยงข้อผิดพลาดจากการประมวลข้อมูล ไม่อนุญาตให้ผู้ใช้งานสร้างโค้ดใหม่ หรือแก้ไขโค้ดของโปรแกรม มีการทบทวนตรวจสอบโค้ดและไลบรารีที่ใช้จากภายนอกเพื่อทบทวนตรวจสอบความจำเป็น และความปลอดภัยมีช่องทางในการปรับปรุงโปรแกรมที่มีความมั่นคงปลอดภัย

สำหรับผู้ที่สนใจรายละเอียดเกี่ยวกับแนวปฏิบัติที่ดีในการพัฒนาโปรแกรมอย่างมั่นคงปลอดภัย สามารถศึกษาข้อมูลเพิ่มเติมได้จากแหล่งข้อมูล และเอกสารดังต่อไปนี้

- Secure Coding Practices, OWASP, https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/

– Secure Software Development Framework (NIST SP 800-218), NIST, https://csrc.nist.gov/Projects/ssdf

9.4. แนวปฏิบัติการจัดการสำหรับการกำหนดค่า (Configuration Management Guideline)

การจัดการการกำหนดค่า (Configuration management) คือกระบวนการในการทำให้การกำหนดค่าขององค์ประกอบของระบบต่าง ๆ ไม่ว่าจะเป็น เซิร์ฟเวอร์ แอปพลิเคชัน อุปกรณ์เครือข่าย หรือสภาพแวดล้อมสารสนเทศอื่น ๆ ถูกจัดเก็บอย่างเป็นระบบ สอดคล้อง และเชื่อถือได้ตลอดวงจรชีวิตของระบบ องค์ประกอบเหล่านี้ล้วนมีการกำหนดค่าเฉพาะที่เกี่ยวข้องกับรุ่น ความมั่นคงปลอดภัย เครือข่าย และอื่น ๆ ที่จำเป็นต่อการทำงานที่เหมาะสม การจัดการกำหนดค่าติดตาม ปรับปรุง และรักษาการกำหนดค่าเหล่านี้ เพื่อให้การทำงานของระบบเป็นไปตามการประเมินพื้นฐาน (Baseline) ที่กำหนดไว้ และมีความมั่นคงปลอดภัยถึงแม้ว่าจะมีการเปลี่ยนแปลงตามเวลาที่ผ่านไป

9.4.1. ความสำคัญของการจัดการการกำหนดค่า

เนื่องจากองค์ประกอบของระบบสารสนเทศต่าง ๆ จำเป็นต้องมีการกำหนดค่าเพื่อให้องค์ประกอบนั้น ๆ สามารถทำงานได้ตามที่ต้องการ แต่ว่าความต้องการของหน่วยงานมักจะมีการเปลี่ยนแปลงไปตามกาลเวลา ทำให้การกำหนดค่าขององค์ประกอบต่าง ๆ จำเป็นต้องมีการเปลี่ยนแปลงตามไปด้วย ระบบสารสนเทศของหน่วยงานมักจะมีองค์ประกอบหลายส่วน และองค์ประกอบเหล่านี้อาจจะเชื่อมต่อ และมีความเกี่ยวข้องกันอย่างซับซ้อน หากไม่มีการจัดการการกำหนดค่าที่ดีอาจทำให้การกำหนดค่าขององค์ประกอบต่าง ๆ เกิดความคลาดเคลื่อนออกจากความต้องการของธุรกิจ และการติดตามแก้ไขอาจทำได้ยาก และมีต้นทุนในการดำเนินการที่สูง

การจัดการการกำหนดค่าช่วยให้สามารถเฝ้าสังเกต และปรับปรุงการกำหนดค่าของระบบตลอดช่วงวงจรชีวิต (Life cycle) ได้ ผู้ใช้สามารถใช้เครื่องมือการจัดการกำหนดค่าอัตโนมัติเพื่อช่วยการดำเนินการเปลี่ยนแปลงได้อย่างปลอดภัย และสม่ำเสมอโดยที่ไม่ต้องดำเนินการปรับปรุงด้วยตนเอง ระบบการจัดการการกำหนดค่าช่วยบันทึกการปรับปรุงที่ผู้ใช้ดำเนินการเพื่อให้ผู้ใช้สามารถวิเคราะห์การเปลี่ยนแปลงที่เกิดขึ้น และประสิทธิภาพของระบบ ช่วยจำแนก และจัดการระบบโดยกลุ่ม และกลุ่มย่อย ช่วยแก้ไขการตั้งค่าฐานจากส่วนกลาง ช่วยดำเนินการการตั้งค่าไปไปที่ระบบที่สามารถใช้งานได้ช่วยระบุ แพทช์ และปรับปรุงระบบโดยอัตโนมัติ ช่วยระบุการกำหนดค่าที่ล้าสมัย ประสิทธิภาพไม่ดี และไม่เป็นไปตามข้อกำหนด ช่วยจัดลำดับความสำคัญของการกระทำ และช่วยการเข้าถึง และการใช้การแก้ไขตามที่กำหนด

การจัดการการกำหนดค่ามีประโยชน์ที่สำคัญดังต่อไปนี้

- ช่วยลดความเสี่ยงของการเกิดระบบขัดข้อง และการละเมิดความมั่นคงปลอดภัยจากการเพิ่มการมองเห็น และการติดตามความเปลี่ยนแปลงของระบบ
- ช่วยลดต้นทุนโดยการมีความรู้ความเข้าใจองค์ประกอบทั้งหมดของการกำหนดค่าหลีกเลี่ยงการทำซ้ำทรัพย์สินทางเทคโนโลยีที่ไม่จำเป็น
- ช่วยให้ลูกค้า และพนักงานได้รับประสบการณ์ที่ดีขึ้นโดยการตรวจจับ และแก้ไขการกำหนดค่าที่ไม่เหมาะสมที่อาจทำให้ประสิทธิภาพของระบบลดลง

- ช่วยควบคุมกระบวนการอย่างเข้มงวดขึ้นโดยการกำหนดและบังคับใช้นโยบายและกระบวนการที่ดูแลการระบุทรัพย์สิน การตรวจสอบสถานะ และการตรวจประเมิน
- ช่วยแก้ปัญหาได้อย่างคล่องตัว และรวดเร็วขึ้น ทำให้สามารถให้บริการที่มีคุณภาพที่ดีขึ้น และลดต้นทุนวิศวกรรมซอฟต์แวร์ (Software Engineering)
- ช่วยเพิ่มประสิทธิภาพในการจัดการการกำหนดค่าโดยรู้จักการกำหนดค่าการประเมินพื้นฐาน (Baseline) และการเพิ่มการมองเห็นซึ่งช่วยให้สามารถออกแบบการเปลี่ยนแปลงที่หลีกเลี่ยงปัญหาที่อาจเกิดขึ้นได้
- ช่วยฟื้นฟูบริการให้กลับสู่สภาพปกติรวดเร็วขึ้นจากการเก็บบันทึกการกำหนดค่าและมีการจัดการการกำหนดค่าแบบอัตโนมัติ
- ช่วยให้การจัดการการเปิดตัวผลิตภัณฑ์ และบริการ และการทำบัญชีสถานะที่ชัดเจน
- ในด้านความมั่นคงปลอดภัย การจัดการการตั้งค่ายังช่วยให้
- ช่วยลดช่องโหว่ความมั่นคงปลอดภัย การกำหนดค่าที่เหมาะสมช่วยปิดช่องว่างและลดช่องโหว่ความมั่นคงปลอดภัย ทำให้ผู้ไม่ประสงค์ดีใช้ประโยชน์จากช่องโหว่ยากขึ้น
- ช่วยให้ระบบเป็นไปตามข้อบังคับ และข้อกำหนดต่าง ๆ ได้ หลายหน่วยงานกำกับและมาตรฐานมีการกำหนดให้มีการกำหนดค่าที่เฉพาะเจาะจง การจัดการการกำหนดค่าจะช่วยให้หน่วยงานสามารถปฏิบัติตามข้อกำหนดเหล่านี้ได้
- ช่วยยกระดับความสอดคล้องต่อเนื่องของระบบ การรักษาการกำหนดค่าขององค์ประกอบต่าง ๆ ของระบบให้มีความสอดคล้องต่อเนื่องกันช่วยให้การจัดการทำได้ง่ายขึ้น และลดความผิดพลาดที่เกิดจากคน
- การตอบสนองต่อเหตุการณ์ที่ไม่คาดคิดสามารถทำได้รวดเร็วขึ้น การรู้จักกับการกำหนดค่าเส้นฐานจะช่วยให้ระบุการเบี่ยงเบนออกจากเส้นฐาน และเหตุการณ์ความมั่นคงปลอดภัยที่อาจเกิดขึ้นได้

9.4.2. แนวทางปฏิบัติที่ดีของการจัดการการกำหนดค่า

เป้าหมายหลักของการจัดการการกำหนดค่าคือการมีกลไกในการเฝ้าระวัง และประเมินการเปลี่ยนแปลงที่กระทำต่อระบบตลอดการพัฒนา และใครได้ดำเนินการเปลี่ยนแปลงเหล่านี้ กระบวนการนี้มีผู้ที่เกี่ยวข้องจากหลายฝ่าย โดยผู้เกี่ยวข้องหลัก ได้แก่

- **นักพัฒนาซอฟท์แวร์ (Software Developer)** มีหน้าที่ในการเขียนโค้ดและดำเนินการการเปลี่ยนแปลงที่ได้รับอนุญาตแล้ว
- **ผู้จัดการการกำหนดค่า (Configuration Manager)** มีหน้าที่ในการระบุว่าใครมีหน้าที่ความรับผิดชอบในเรื่องใด ดำเนินการให้แต่ละคนปฏิบัติตามขั้นตอนที่กำหนดไว้ตลอดช่วงระยะเวลาดำเนินโครงการ และเป็นผู้ตัดสินคนสุดท้ายในการร้องขอการเปลี่ยนแปลงแก้ไข

- **ผู้จัดการโครงการ (Project Manager)** มีหน้าที่กำหนดแผนการดำเนินการโครงการเพื่อให้โครงการเสร็จสิ้นตามระยะเวลาของโครงการที่กำหนดไว้ และรายงานความก้าวหน้าการดำเนินการของทีม นอกจากนี้ผู้จัดการโครงการจะต้องทำให้สมาชิกโครงการปฏิบัติตามขั้นตอนในการสร้าง แก้ไข และทดสอบโปรแกรม

- **ผู้ตรวจสอบ (Auditor)** ทำหน้าที่ในการตรวจสอบ และทบทวนระบบเวอร์ชันสุดท้ายว่ามีความสอดคล้อง ถูกต้อง ครบถ้วนหรือไม่

ผู้ที่เกี่ยวข้องควรดำเนินการขั้นตอนดังต่อไปนี้

1) **การวางแผนงาน และการระดมสมอง** การจัดการการกำหนดค่าเริ่มต้นที่จุดเริ่มต้นของโครงการเมื่อเริ่มวางแผนกลยุทธ์การจัดการโครงการ เป้าหมายคือการวางแผนวิวัฒนาการของระบบและกำหนดขอบเขต การไปถึงเป้าหมายนี้สามารถทำได้โดยการจัดการประชุม อภิปราย และระดมสมองกับทีมเพื่อกำหนดความต้องการพื้นฐานตลอดระยะเวลาโครงการ มีการกำหนด และบันทึกกระบวนการและกลยุทธการจัดการการกำหนดค่าเพื่อให้ทุกคนรู้ว่าอะไรจะเกิดขึ้นเมื่อใด และอะไรคือสิ่งที่คาดหวังไว้

2) **การระบุรายการกำหนดค่า งาน และสิ่งส่งมอบ** มีการกำหนดรหัสเฉพาะแต่ละรายการกำหนดค่าเพื่อให้สามารถติดตามได้ ผู้จัดการโครงการมีความรับผิดชอบสูงสุดในการจัดการการกำหนดค่าถึงแม้ว่าบุคคลอื่นอาจจะเป็นผู้ดูแลแมทริกซ์การติดตาม และการควบคุมเวอร์ชัน กระบวนการนี้รวมถึงการกำหนดความก้าวหน้าของโครงการ และกำหนดข้อกำหนดความสมบูรณ์ของโครงการ บุคคลในทีมจะสามารถตรวจสอบได้ว่าสามารถบรรลุวัตถุประสงค์ของโครงการได้ครบถ้วน หรือไม่ ตัวอย่างรายการกำหนดค่า เช่น เอกสารโครงการ กรณีทดสอบ ข้อกำหนด และโมดูลโค้ด

3) **การจัดทำการประเมินพื้นฐาน (Baseline)** เทคโนโลยีการจัดการการกำหนดค่าส่วนมากจะทำการสแกนสภาพแวดล้อมสารสนเทศ และให้ข้อมูลที่จำเป็นในการจัดทำเส้นฐานการจัดการการกำหนดค่า เส้นฐานการจัดการการกำหนดค่าดังกล่าวคือกลุ่มของการตั้งค่าระบบที่คงที่ใช้สำหรับการตรวจสอบความเปลี่ยนแปลงที่เกิดขึ้น การกำหนดเส้นฐานช่วยรับรองความครบถ้วนสมบูรณ์ของผลิตภัณฑ์ด้วยการกำหนดเวอร์ชันของซอฟท์แวร์ที่เป็นที่ยอมรับ เมื่อโครงการมีการดำเนินไปการประเมินพื้นฐาน (Baseline) ใหม่ก็จะมีการถูกจัดทำขึ้นใหม่ ทำให้เกิดซอฟท์แวร์หลายเวอร์ชันได้

4) **การควบคุมการเปลี่ยนแปลง และการจดบันทึกรายละเอียด** การควบคุมการเปลี่ยนแปลงคือกระบวนการที่ช่วยรับรองได้ว่าการเปลี่ยนแปลงที่เกิดขึ้นจะสามารถเข้ากันได้กับโครงการที่เหลืออยู่ เป็นการควบคุมคุณภาพ และการสร้างข้อมูลการประเมินพื้นฐาน (Baseline) ในขั้นตอนนี้ จะมีการนำเสนอคำร้องขอเปลี่ยนแปลงการกำหนดค่าต่อทีม และมีการพิจารณาอนุญาต หรือปฏิเสธโดยผู้ดูแลการกำหนดค่า การเพิ่ม หรือแก้ไขรายการกำหนดค่า หรือการเปลี่ยนแปลงสิทธิของผู้ใช้คือคำร้องขอที่พบได้บ่อย นอกจากนี้ บันทึกการกำหนดค่าควรมีการควบคุมดูแลอย่างเข้มงวดเพื่อสามารถใช้เป็นเส้นทางการตรวจสอบตั้งแต่ความต้องการเริ่มต้นจนถึงเวอร์ชันสุดท้าย

5) การรักษาความรับผิดชอบต่อสถานะรายการ มีการตรวจสอบว่าโครงการได้ดำเนินไปตามแผนงานที่วางไว้โดยการทดสอบ และประเมินเปรียบเทียบกับการประเมินพื้นฐาน (Baseline) ที่ได้กำหนดไว้ ความรับผิดชอบสถานะการกำหนดค่าจะต้องสังเกตการณ์แต่ละเวอร์ชันที่เกิดขึ้นในกระบวนการ ตรวจสอบว่ามีอะไรใหม่ในแต่ละเวอร์ชัน และทำไมต้องมีการเปลี่ยนแปลง ทีมควรจะสามารถบอกได้ว่าวัตถุประสงค์ต่าง ๆ อยู่ในสถานะมีผลอยู่ สมบูรณ์ มีการนำออก หรือสถานะอื่น ๆ ตามที่กำหนด รวมถึงใครเป็นผู้ดำเนินการการสังเกตการณ์กระบวนการ และการเสร็จสิ้นของคำร้องขอเปลี่ยนแปลงถือเป็นส่วนหนึ่งของขั้นตอนนี้ ทีมจะต้องสามารถให้ข้อมูลเกี่ยวกับทรัพย์สินของโครงการโดยบอกได้ว่าแต่ละรายการมีความพร้อมใช้งาน หรือไม่ และอยู่ที่ใด นอกจากนี้ยังรวมถึงสถานะทางการเงิน เช่น รายจ่าย งบประมาณ และค่าเสื่อมราคา

6) การตรวจสอบ การตรวจสอบช่วยให้สามารถตรวจสอบได้ว่ารายการกำหนดค่าเป็นไปตามการกำหนดค่าที่คาดหวังไว้ หลายความพยายามในการจัดการการกำหนดค่าพบปัญหาเมื่อไม่สามารถติดตามทรัพย์สินที่จับต้องได้ เช่น วัสดุ โค้ด หรือทรัพย์สินการกำหนดค่าอื่น ๆ หรือเมื่อลักษณะของสิ่งส่งมอบมีการเบี่ยงเบนออกจากสิ่งที่คาดหวังไว้ ขั้นตอนการตรวจสอบช่วยให้การกำหนดค่าเป็นไปตามที่ระบุไว้

7) การจดบันทึก และการฝึกอบรม มีการจัดทำเอกสารกระบวนการการจัดการการกำหนดค่า และฝึกอบรมพนักงานให้เข้าใจ และสามารถปฏิบัติตามขั้นตอน และกระบวนการการจัดการการกำหนดค่าที่เหมาะสมได้

สำหรับผู้ที่สนใจรายละเอียดเกี่ยวกับแนวปฏิบัติที่ดีในการจัดการการกำหนดค่า สามารถศึกษาข้อมูลเพิ่มเติมได้จากแหล่งข้อมูล และเอกสารดังต่อไปนี้

- What Is Configuration Management and Why Is It Important, UpGuard, https://www.upguard.com/blog/5-configuration-management-boss
- What Is Configuration Management? Working, Tools, and Importance, Spiceworks, https://www.spiceworks.com/tech/devops/articles/what-is-configuration-management/
- Guide for Security-Focused Configuration Management of Information Systems (NIST SP 800-128), NIST, https://csrc.nist.gov/pubs/sp/800/128/upd1/final

9.5. แนวปฏิบัติการป้องกัน และรับมือแรนซัมแวร์ (Ransomware Protection/Response Guideline)

แรนซัมแวร์ (Ransomware) หรือมัลแวร์เรียกค่าไถ่ คือ มัลแวร์ประเภทหนึ่งที่มีพฤติกรรมขัดขวางไม่ให้ผู้ใช้สามารถเข้าถึงข้อมูลที่อยู่บนระบบคอมพิวเตอร์ได้ และมีการเรียกค่าไถ่เพื่อให้ผู้ใช้สามารถเข้าถึงข้อมูลได้อีกครั้ง ซึ่งแตกต่างจากมัลแวร์ประเภทอื่น ๆ ที่อาจมุ่งเน้นการทำลาย หรือโจรกรรมข้อมูลเพียงอย่างเดียว เทคนิคในการขัดขวางไม่ให้ผู้ใช้เข้าถึงไฟล์แบ่งออกเป็น 3 วิธีหลัก ดังนี้

1) การล็อคหน้าจอของอุปกรณ์ วิธีนี้มัลแวร์จะทำการทำการล็อคหน้าจอ เช่น การแสดงหน้าจอปิดบังไม่ให้ผู้ใช้เข้าถึงหน้าจอหลักของอุปกรณ์ได้ โดยอาจจะไม่มีการเข้ารหัสลับข้อมูลใด ๆ ดังนั้นผู้ใช้อาจยังสามารถเข้าถึงข้อมูลได้ด้วยวิธีการบายพาสหน้าจอที่ถูกล็อคได้

2) การเข้ารหัสลับเฉพาะไฟล์เป้าหมาย วิธีนี้มัลแวร์จะเข้ารหัสลับข้อมูลไฟล์ที่สำคัญของผู้ใช้ที่เก็บอยู่บนคอมพิวเตอร์ หรือที่เก็บข้อมูลภายนอก เช่น คลาวด์ ซึ่งเครื่องคอมพิวเตอร์มักจะยังสามารถใช้งานได้เพียงแต่ไม่สามารถเข้าถึงไฟล์ข้อมูลที่ถูกเข้ารหัสลับได้

3) การเข้ารหัสลับทั้งดิสก์ วิธีนี้มัลแวร์จะเข้ารหัสลับข้อมูลทั้งดิสก์ ทำให้ผู้ใช้ไม่สามารถเปิดระบบปฏิบัติการ หรือเข้าถึงข้อมูลที่อยู่บนดิสก์นั้นได้ ทั้งหมด

ซึ่งหลังจากที่แรนซัมแวร์ทำการขัดขวางไม่ให้ผู้ใช้เข้าถึงไฟล์ได้แล้ว แรนซัมแวร์มักจะแสดงข้อความเรียกค่าไถ่เพื่อแลกกับการปลดล็อคหน้าจอ หรือกุญแจถอดรหัสลับเพื่อให้ได้ข้อมูลคืนมา นอกจากนี้ยังอาจจะมีการขู่เรียกค่าไถ่เพิ่มเพื่อแลกกับการไม่เปิดเผยข้อมูลสู่สาธารณะ หรือแม้กระทั้งในกรณีที่ผู้ใช้ยินยอมจ่ายค่าไถ่ทั้งหมดแล้ว ผู้โจมตีก็อาจจะยังนำข้อมูลผู้ใช้ไปประมูลขายในตลาดมืด

ช่องทางการแพร่กระจายของแรนซัมแวร์โดยทั่วไปแบ่งได้ดังนี้

1) อีเมลที่ส่งมาจากผู้โจมตี โดยทั่วไปจะมีไฟล์แนบอันตรายมาด้วย หรือมีลิงค์ไปยังเว็บไซต์ที่มีไฟล์อันตรายให้ดาวน์โหลด เมื่อผู้ใช้เปิดไฟล์อันตรายดังกล่าวแรนซัมแวร์จะทำงาน และทำการปกป้องผู้ใช้จากการเข้าถึงไฟล์ข้อมูล

2) การเปิดเว็บไซต์ และดาวน์โหลดไฟล์อันตราย ซึ่งผู้ใช้อาจไปพบเว็บไซต์อันตรายจากช่องทางต่าง ๆ เช่น โฆษณาแอบอ้าง เว็บไซต์ปลอม และลิงค์จากเว็บไซต์ที่ไม่น่าเชื่อถือ หรือถูกแฮ็ก ซึ่งเมื่อผู้ใช้เปิดเว็บไซต์ และดาวน์โหลดไฟล์อันตรายโดยที่รู้ตัว หรือไม่รู้ตัว ไฟล์จะถูกเปิด และทำให้แรนซัมแวร์ทำงานได้

3) การดาวน์โหลด และใช้งานแอปพลิเคชันเถื่อน ผิดลิขสิทธิ์ ซึ่งอาจมีแรนซัมแวร์ฝังอยู่ในแอปพลิเคชันเถื่อนเหล่านั้น เมื่อผู้ใช้เปิดก็จะถูกล็อคไม่ให้เข้าถึงไฟล์ข้อมูล

4) การโจมตีโดยใช้ช่องโหว่ของเครื่องในการแพร่กระจายแรนซัมแวร์ซึ่งอาจจะกระทำโดยการสร้างเว็บไซต์อันตราย และเมื่อผู้ใช้เข้ามาเว็บไซต์ดังกล่าวก็จะถูกโจมตีโดยไม่รู้ตัว หรือผู้โจมตีอาจจะเจาะระบบเข้าเซิร์ฟเวอร์เพื่อติดตั้งแรนซัมแวร์ และล็อคไฟล์ข้อมูลบนเครื่อง

9.5.1. แนวทางการป้องกัน

แนวทางการป้องกันการถูกโจมตีด้วยแรนซัมแวร์เบื้องต้นสำหรับผู้ใช้งานทั่วไปมีดังต่อไปนี้

1) ใช้งานซอฟท์แวร์ที่ถูกลิขสิทธิ์ มาจากแหล่งที่เชื่อถือได้ ใช้งานเฉพาะซอฟท์แวร์ที่จำเป็น ไม่ใช้งานซอฟท์แวร์เถื่อน หรือมาจากแหล่งที่ไม่น่าเชื่อถือ เพื่อลดโอกาสเสี่ยงการโหลดแอปพลิเคชันที่มีแรนซัมแวร์แอบแฝงมาด้วย

2) อัปเดตซอฟท์แวร์ให้เป็นปัจจุบันทั้งระบบปฏิบัติการ และแอปพลิเคชันต่าง ๆ โดยเฉพาะเมื่อมีแพทช์การปรับปรุงแก้ไขช่องโหว่ความมั่นคงปลอดภัย เพื่อลดความเสี่ยงจากการถูกใช้ประโยชน์จากช่องโหว่ความมั่นคงปลอดภัยในการติดตั้ง และรันแรนซัมแวร์

3) ไม่เปิดเว็บไซต์ คลิกลิงค์ที่ไม่น่าเชื่อถือ ไม่เปิดไฟล์แนบที่น่าสงสัย หรือมาจากอีเมลที่ไม่น่าไว้ใจ เพื่อลดความเสี่ยงจากการเปิดเว็บไซต์ และไฟล์อันตราย

4) ไม่เชื่อมต่ออุปกรณ์ เช่น แฟลชไดรฟ์ และฮาร์ดดิสก์พกพา ที่ไม่คุ้นเคย หรือไม่น่าเชื่อถือเข้ากับเครื่องคอมพิวเตอร์

5) ติดตั้งแอปพลิเคชันป้องกันมัลแวร์ และอัปเดตแอปพลิเคชัน และฐานข้อมูลให้เป็นปัจจุบันอยู่เสมอ เพื่อป้องกัน และตรวจจับแรนซัมแวร์ ลดความเสี่ยงจากการถูกโจมตีได้

6) สำหรับหน่วยงาน ควรมีการสแกน และตรวจสอบไฟล์แนบ และลิงค์ที่ส่งมายังอีเมลของพนักงานในหน่วยงานก่อนจะส่งต่ออีเมลนั้น ๆ ไปยังพนักงานในหน่วยงาน เพื่อลดโอกาสที่พนักงานจะคลิกลิงค์อันตราย หรือไฟล์น่าสงสัย

7) ทำการสำรองข้อมูลอย่างสม่ำเสมอ ควรมีการทำสำเนาไว้หลายสื่อเก็บข้อมูล มีการสแกนมัลแวร์ในข้อมูลสำรอง และทดสอบว่าสามารถกู้คืนข้อมูลสำรองมาใช้ได้ หรือไม่ จะช่วยลดผลกระทบความเสียหายจากการถูกล็อคไม่ให้เข้าถึงข้อมูลผู้ใช้จะยังสามารถกู้คืนข้อมูลที่มีการสำรองล่าสุดได้

8) เก็บข้อมูลที่มีความละเอียดอ่อนเท่าที่จำเป็น ในระยะเวลาที่เหมาะสม และมีการปกป้องการเข้าถึงอย่างเหมาะสม เช่น มีการเข้ารหัสลับข้อมูลลับ เพื่อลดความเสี่ยง และผลกระทบจากการถูกนำข้อมูลไปเปิดเผย หรือข้อมูลรั่วไหล

9) มีการตั้งค่าความมั่นคงปลอดภัยของระบบเพื่อป้องกันการโจมตีอย่างเหมาะสม มีการใช้การพิสูจน์ตัวตนที่มั่นคงปลอดภัย ควรใช้การพิสูจน์ตัวตนหลายปัจจัยก่อนเข้าถึงระบบ หรือข้อมูลที่มีความละเอียดอ่อน และมีการตรวจสอบสถานะของเครื่องเป็นประจำ

สำหรับผู้ดูแลระบบในหน่วยงาน แนวทางการป้องกัน บรรเทาผลกระทบ และรับมือแรนซัมแวร์เบื้องต้นมีดังต่อไปนี้

1) ปรับปรุงให้ระบบปฏิบัติการ และแอปพลิเคชันที่ติดตั้งอยู่บนอุปกรณ์ของหน่วยงานทันสมัยอยู่เสมอ ควรมีการติดตั้งแพทช์ปรับปรุงความมั่นคงปลอดภัยให้เป็นปัจจุบัน พิจารณาการเปิดฟังก์ชันการอัพเดตอัตโนมัติ อาจมีการพิจารณาใช้การบริหารจัดการแพทช์จากส่วนกลาง

2) รู้ว่าภายในหน่วยงานมีทรัพย์สินอะไรบ้าง และแบ่งกลุ่มอย่างเหมาะสม โดยเฉพาะข้อมูลที่มีความละเอียดอ่อนควรมีการเก็บแยกจากข้อมูลทั่วไปที่ไม่เป็นความลับ มีการแบ่งแยกโซนเครือข่ายเพื่อลดความเสี่ยง และความเสียหายที่อาจเกิดขึ้นหากอุปกรณ์ในเครือข่ายถูกโจมตี

3) มีการควบคุมการเข้าถึงจากทางไกลอย่างมั่นคงปลอดภัย หากมีความจำเป็นต้องให้เข้าถึงระบบ และทรัพยากรของหน่วยงานจากนอกหน่วยงานได้ ควรมีการประเมินความเสี่ยง และใช้มาตรการการรักษาความมั่นคงปลอดภัยอย่างเหมาะสม

4) เฝ้าระวังการโจรกรรมข้อมูล การโจมตีด้วยแรนซัมแวร์ในหลายกรณีมีการขู่ว่าจะมีการเปิดเผยข้อมูลของหน่วยงานสู่สาธารณะ หากสามารถตรวจจับการโจรกรรมข้อมูลได้รวดเร็วเท่าไรก็จะสามารถลดความเสียหายได้มากขึ้นเท่านั้น

5) ประเมิน และทดสอบระบบอย่างสม่ำเสมอ รวมถึงการประเมิน และทดสอบความมั่นคงปลอดภัยของระบบ และการทดสอบการสำรองข้อมูล และกู้คืนข้อมูลจากข้อมูลที่ได้สำรองไว้ เพื่อให้มั่นใจได้ว่าสามารถกู้คืนข้อมูลได้ในกรณีที่เกิดเหตุขึ้น

6) ลดความน่าจะเป็นที่ข้อมูลอันตรายจะเข้าสู่ระบบเครือข่ายของหน่วยงาน ปิดการใช้งานฟังก์ชัน สคริปต์ และแมโครที่ไม่จำเป็น มีการตั้งค่าอุปกรณ์ในเครือข่ายให้มีการกรองข้อมูลบางประเภทที่ไม่ใช้งาน หรือมีความเสี่ยงสูง มีการตรวจสอบ และกรองข้อมูลเครือข่ายที่เข้าออกเครือข่ายหน่วยงาน มีการใช้ข้อมูลภัยคุกคาม (Threat intelligence) จากแหล่งที่เชื่อถือได้ และเป็นปัจจุบัน

7) ใช้รหัสผ่านที่มีความมั่นคงปลอดภัย และมีการใช้การพิสูจน์ตัวจริงที่มีความแข็งแรง มีการใช้อักษรตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข สัญลักษณ์พิเศษผสมกัน และมีความยาวที่เหมาะสม คาดเดาได้ยาก สร้างความตระหนักให้กับพนักงานให้เห็นความสำคัญของการใช้รหัสผ่านที่มีความมั่นคงปลอดภัย นอกจากนี้การเข้าถึงระบบ และทรัพยากรที่มีความสำคัญ ควรพิจารณาใช้การพิสูจน์ตัวจริงหลายปัจจัย

8) จัดการการใช้งานงานบัญชีที่มีสิทธิสูง ควรจำกัดสิทธิบัญชีของพนักงานในหน่วยงานทั่วไปในการติดตั้งแอปพลิเคชันบนอุปกรณ์ที่เชื่อมต่อกับเครือข่ายองค์กร จำกัดการใช้งานบัญชีที่มีสิทธิสูงตามบทบาทหน้าที่ที่จำเป็น ใช้หลักการสิทธิพิเศษขั้นต่ำในการปฏิบัติงาน หลักการรู้เท่าที่จำเป็น และการแบ่งแยกหน้าที่

9) ติดตั้งแอปพลิเคชันที่มาจากแหล่งที่เชื่อถือได้เท่านั้น หากมีความจำเป็นหน่วยงานอาจพิจารณาพัฒนาแพลตฟอร์มเพื่อให้ดาวน์โหลดแอปพลิเคชันที่ได้รับการรับรองจากหน่วยงานเพื่อใช้ภายใน

10) อบรม และให้ความรู้กับพนักงานในหน่วยงาน ให้พนักงานมีความตระหนัก และเห็นความสำคัญของการรักษาความมั่นคงปลอดภัย ให้ความรู้เกี่ยวกับนโยบาย และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของหน่วยงานโดยเฉพาะเรื่องฟิชชิง และโซเชียลเอนจิเนียริง ควรมีการจำลองฟิชชิงเพื่อทดสอบ และเสริมสร้างความตระหนักรู้ของพนักงาน มีช่องทางในการแจ้งเหตุให้กับพนักงาน และควรมีวิธีการสร้างขวัญ และกำลังใจให้พนักงานมีส่วนร่วม เช่น ป๊อปอัพแสดงข้อความขอบคุณ หรือการสะสมคะแนน

11) ควรมีการวางแผนการรับมือเมื่อเกิดเหตุถูกโจมตีด้วยแรนซัมแวร์ขึ้น ให้ผู้ใช้งานรู้กระบวนการว่าจะต้องทำอย่างไร แจ้งใคร และผู้ดูแลระบบรู้ว่าต้องดำเนินการอย่างไปเพื่อทำการตรวจสอบ จำกัดขอบเขตความเสียหาย กำจัดแรนซัมแวร์ (Ransomware) กู้คืนข้อมูล และถอดบทเรียนเพื่อปรับปรุง และป้องกันการโจมตีครั้งถัดไป

แนวทางการสำรองและกู้คืนข้อมูลเพื่อลดผลกระทบจากแรนซัมแวร์

การป้องกันและรับมือกับแรนซัมแวร์จำเป็นจะต้องใช้หลายมาตรการควบคู่กันเพื่อให้ได้ประสิทธิภาพในการปกป้องที่ดีและลดผลกระทบจากการโจมตีโดยแรนซัมแวร์ หนึ่งในขั้นตอนสำคัญที่ช่วยปกป้องข้อมูลไม่ให้เกิดความเสียหายและสามารถกู้คืนข้อมูลได้คือการสำรองและกู้คืนข้อมูล ทั้งนี้กระบวนการสำรองและกู้คืนข้อมูลที่ไม่เหมาะสมอาจไม่สามารถป้องกันการโจมตีจากแรนซัมแวร์ได้และอาจทำให้ผู้ใช้เข้าใจผิดว่าตนเองปลอดภัยจากการโจมตีโดยแรนซัมแวร์แล้ว เช่น การสำรองข้อมูลทั้งหมดโดยที่ไม่ตรวจสอบว่าข้อมูลสำรองมีแรนซัมแวร์ติดไปด้วยหรือไม่ หรือการกู้คืนข้อมูลจากข้อมูลล่าสุดที่ถูกเข้ารหัสโดยแรนซัมแวร์แล้ว แนวทางการสำรองและกู้คืนข้อมูลที่ดีเบื้องต้นมีดังต่อไปนี้

1. มีการตรวจสอบข้อมูล ทั้งข้อมูลก่อนการสำรองและข้อมูลที่เก็บสำรองไว้แล้ว ว่าไม่มีการติดมัลแวร์โดยเฉพาะแรนซัมแวร์ ควรมีระบบตรวจสอบมัลแวร์ที่เครื่องผู้ใช้ และเซิร์ฟเวอร์ที่จัดเก็บข้อมูลสำรอง

2. ควรทำข้อมูลสำรองหลายชุด แยกเก็บกระจายหลายสื่อ หลายพื้นที่ และควรมีอย่างน้อย 1 ชุดที่เก็บแบบออฟไลน์ ไม่เชื่อมต่อกับระบบออนไลน์ใด ๆ หรือมีการเชื่อมต่อเท่าที่จำเป็นเท่านั้น

3. อาจพิจารณาใช้สื่อเก็บข้อมูลแบบเขียนครั้งเดียวอ่านหลายครั้ง (Write-Once-Read-Many) หรือ Immutable storage เมื่อมีการสำรองข้อมูลที่ปลอดจากมัลแวร์แล้ว มัลแวร์จะไม่สามารถทำการแก้ไขข้อมูลได้อีก

4. มีการทำแม่แบบระบบที่พร้อมใช้งาน (Gold Image) ของระบบที่สำคัญ ซึ่งแม่แบบนี้มีซอฟท์แวร์และการตั้งค่าของระบบที่พร้อมใช้งาน ซึ่งจะช่วยให้ผู้ดูแลระบบสามารถกู้คืนระบบกลับมาให้อยู่ในสภาพพร้อมใช้งานได้อย่างรวดเร็ว

5. มีการทดสอบการกู้คืนข้อมูล และก่อนการกู้คืนข้อมูลควรมีการตรวจสอบให้แน่ใจว่าไม่มีมัลแวร์ปนอยู่ในข้อมูล และข้อมูลสำรองนั้นไม่ได้ถูกเข้ารหัสลับไปแล้วการทดสอบการกู้คืนข้อมูลควรทำในระบบทดสอบก่อนที่จะใช้งานกับระบบจริง

9.5.2. แนวทางการรับมือ และการตอบสนอง

แนวทางการรับมือ และการตอบสนองเบื้องต้นสำหรับผู้ใช้งานทั่วไปในกรณีที่พบว่าถูกโจมตีด้วยแรนซัมแวร์มีดังต่อไปนี้

1) สังเกตว่ามีแอปพลิเคชัน หรือโปรเซสที่ไม่รู้จัก หรือน่าสงสัยบนเครื่อง หรือไม่ หากมีและแอปพลิเคชัน หรือโปรเซสดังกล่าวกำลังทำงานอยู่ และใช้ทรัพยากรของเครื่องอย่างหนัก ให้ตัดการเชื่อมต่ออินเตอร์เน็ตของเครื่อง (ไม่ว่าจะเป็นการเชื่อมต่อแบบมีสาย หรือไร้สาย) เพื่อป้องกันการแพร่กระจายไปยังเครื่องอื่น ๆ ในเครือข่าย

2) ถ่ายรูป เก็บภาพ หรือข้อความเรียกค่าไถ่ไว้เพื่อเป็นข้อมูลอ้างอิง และเป็นหลักฐาน

3) ถ้ามีแอปพลิเคชันแอนตี้ไวรัส หรือแอนตี้มัลแวร์ ควรใช้แอปพลิเคชันนั้นสแกนเครื่องเพื่อกำจัดแรนซัมแวร์ออกจากเครื่องด้วย ทั้งนี้อาจจะต้องรีสตาร์ทเครื่องเข้าสู่เซฟโหมด

4) การลบแรนซัมแวร์ออกจากเครื่องไม่ได้เป็นการถอดรหัสไฟล์ หรือกู้คืนไฟล์ที่ถูกล็อคไปคืนมา แต่ว่าจะเป็นการหยุดการล็อคไฟล์ใหม่เพิ่มเติม และสามารถดำเนินการขั้นตอนต่อไปได้

5) ถ้ามีข้อมูลที่ได้สำรองไว้ ทำการกู้คืนข้อมูลจากข้อมูลสำรอง และดำเนินการเพื่อป้องกันการถูกโจมตีด้วยแรนซัมแวร์อีก

6) ถ้าหากไม่มีข้อมูลที่สำรองไว้ ให้ไปที่เว็บไซต์ https://www.nomoreransom.org/ [7] เพื่อตรวจสอบว่าแรนซัมแวร์ที่ติดเครื่องเป็นหนึ่งในสายพันธุ์ที่มีเครื่องมือในการปลดล็อคข้อมูลคืนมา หรือไม่ ซึ่งเครื่องมือเหล่านี้สามารถใช้งานได้โดยไม่มีค่าใช้จ่าย ข้อมูลที่เกี่ยวข้องกับแรนซัมแวร์ที่ได้เก็บบันทึกไว้ก่อนหน้าจะช่วยให้การค้นหา และพิจารณาทำได้สะดวกขึ้น

7) แจ้งข้อมูลกับหน่วยงานที่เกี่ยวข้องเพื่อให้สามารถดำเนินการในส่วนที่เกี่ยวข้องต่อไป และมีการเตรียมตัวรับมือกับการโจมตีที่อาจเกิดขึ้นในอนาคต

ในกรณีที่พบการติด และถูกโจมตีโดยแรนซัมแวร์ ผู้ดูแลระบบควรดำเนินการดังต่อไปนี้

1) ตัดการเชื่อมต่อจากระบบเครือข่ายทุกช่องทาง ไม่ว่าจะเป็นแบบมีสาย หรือไร้สาย ทั้งนี้ไม่ควรปิดเครื่องนั้น ๆ โดยทันทีเพราะอาจทำให้หลักฐาน และร่องรอยการโจมตีสูญหายได้ เว้นแต่ประเมินความเสี่ยงแล้วมีความจำเป็นต้องดำเนินการปิดเครื่อง

2) ในกรณีที่มีความรุนแรงมาก อาจพิจารณาปิดเครือข่ายหลักของหน่วยงาน หรือแม้กระทั้งการเชื่อมต่อกับอินเตอร์เน็ตเพื่อช่วยควบคุมการแพร่กระจาย

3) มีการเปลี่ยนข้อมูลการพิสูจน์ตัวจริง โดยเฉพาะบัญชีผู้ดูแลระบบ แต่ต้องมั่นใจว่ายังสามารถเข้าใช้งานระบบสำคัญที่จำเป็นต่อการกู้คืนระบบ และข้อมูลได้

4) รายงานเหตุที่เกิดขึ้นให้กับหน่วยงานที่เกี่ยวข้องเพื่อดำเนินการต่อ

5) เก็บหลักฐานที่เกี่ยวข้องตามคำแนะนำของหน่วยงานที่มีอำนาจหน้าที่ในการสืบสวนสอบสวนเหตุการโจมตีด้วยแรนซัมแวร์ เช่น การสร้างอิเมจไฟล์ การเก็บข้อมูลใน RAM และการเก็บล็อก

6) กำจัดแรนซัมแวร์ ทำความสะอาดเครื่อง และติดตั้งระบบปฏิบัติการ และแอปพลิเคชันของเครื่องที่ได้รับผลกระทบใหม่

7) ก่อนการกู้คืนข้อมูลจากข้อมูลสำรอง ตรวจสอบให้มั่นใจว่าข้อมูลสำรองปลอดจากมัลแวร์ และสะอาด

8) เชื่อมต่ออุปกรณ์กับเครือข่ายที่ปลอดภัยเพื่อดาวน์โหลด และติดตั้งอัปเดต และแพทช์

9) ติดตั้ง และใช้งานแอปพลิเคชันแอนตี้มัลแวร์

10) เชื่อมต่อกับเครือข่ายที่ใช้งานปกติ

[7] เว็บไซต์ “No More Ransom” เป็นโครงการที่เกิดจากความร่วมมือระหว่าง National High Tech Crime Unit of the Netherlands’ police, Europol’s European Cybercrime Centre, Kaspersky, และ McAfee โดยมีเป้าหมายที่จะช่วยเหลือเหยื่อแรนซัมแวร์ให้สามารถกู้คืนข้อมูลที่ถูกล็อคโดยไม่ต้องเสียค่าใช้จ่ายให้กับผู้โจมตี

11) ตรวจสอบ และเฝ้าระวังข้อมูลที่ส่งผ่านเครือข่าย และรันสแกนบนเครื่องเพื่อดูว่ามีร่องรอยการติดมัลแวร์หลงเหลืออยู่ หรือไม่

สำหรับผู้ที่สนใจรายละเอียดเกี่ยวกับแนวปฏิบัติที่ดีในการป้องกัน และรับมือแรนซัมแวร์ สามารถศึกษาข้อมูลเพิ่มเติมได้จากแหล่งข้อมูล และเอกสารดังต่อไปนี้

- Stop Ransomware, CISA, https://www.cisa.gov/stopransomware
- How to prevent a ransomware attack, No More Ransom, https://www.nomoreransom.org/en/prevention-advice.html
- What is Ransomware and What You Need to Know to Stay Safe, Bitdefender, https://www.bitdefender.com/blog/hotforsecurity/what-is-ransomware-and-what-you-need-to-know-to-stay-safe/

9.6. แนวปฏิบัติการเสริมความมั่นคงปลอดภัยแอปพลิเคชัน และระบบปฏิบัติการ (Application & Operating System Hardening)

แอปพลิเคชัน (Application) หรือ โปรแกรม (Program) เป็น ซอฟท์แวร์กลุ่มหนึ่งที่ถูกออกแบบมาเพื่อดำเนินงานเฉพาะวัตถุประสงค์ นอกเหนือจากการทำงานปกติของเครื่องคอมพิวเตอร์ โดยทั่วไปแอปพลิเคชันถูกพัฒนาเพื่อการใช้งานตามความต้องการของผู้ใช้ เช่น แอปพลิเคชันประมวลผลคำ แอปลิเคชันเล่นสื่อบันเทิง และแอปพลิเคชันเปิดเว็บ

ระบบปฏิบัติการ (Operating system) คือ ซอฟท์แวร์ระบบที่ใช้ในการบริหารจัดการทรัพยากรฮาร์ดแวร์และซอฟท์แวร์ของเครื่องคอมพิวเตอร์ กล่าวคือ ระบบปฏิบัติการเป็นตัวกลางระหว่างแอปพลิเคชันและฮาร์ดแวร์ ก่อนที่แอปพลิเคชันจะเข้าถึงฮาร์ดแวร์ต่าง ๆ ไม่ว่าจะเป็นหน่วยนำเข้าข้อมูล เช่น คีย์บอร์ดและเมาส์ หน่วยเก็บข้อมูล เช่น RAM และฮาร์ดดิสก์ จะต้องผ่านการจัดสรรทรัพยากรโดยระบบปฏิบัติการ

ถึงแม้ว่าผู้พัฒนาซอฟท์แวร์ที่มีประสบการณ์และน่าเชื่อถือจะมีการออกแบบและทดสอบซอฟท์แวร์อย่างเข้มงวดก่อนปล่อยซอฟท์แวร์ดังกล่าวสู่ตลาด ซอฟท์แวร์เหล่านี้ก็ยังคงมีช่องโหว่ความมั่นคงปลอดภัยที่หลุดรอดจากการทดสอบหรือเป็นช่องโหว่ความมั่นคงปลอดภัยใหม่ที่ไม่เคยมีใครรู้จักมาก่อน ผู้พัฒนาซอฟท์แวร์บางกลุ่มอาจจะไม่ให้ความสำคัญกับการทดสอบซอฟท์แวร์อย่างเพียงพอ โดยเน้นเฉพาะฟังก์ชันการทำงาน และเวลาที่ต้องปล่อยซอฟท์แวร์สู่ตลาดก่อนคู่แข่งเพื่อแย่งชิงความได้เปรียบ ทำให้ผู้ไม่ประสงค์ดีสามารถใช้ช่องโหว่ความมั่นคงปลอดภัยเหล่านี้ในการเข้าสู่ระบบและเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และอาจสร้างความเสียหายในรูปแบบต่าง ๆ ได้อย่างมหาศาล นอกจากนี้ เนื่องจากผู้พัฒนาต้องการซอฟท์แวร์ตอบสนองความต้องการและเข้าถึงกลุ่มผู้ใช้ที่มีความต้องการที่หลากหลาย ทำให้การตั้งค่าเริ่มต้นในการใช้งานจะมุ่งเน้นไปที่ความสะดวกในการใช้งานมากกว่าการรักษาความมั่นคงปลอดภัยที่เข้มงวด ซึ่งอาจจะเป็นช่องทางให้ผู้ไม่ประสงค์ดีใช้ประโยชน์ได้

ดังนั้นผู้พัฒนาและผู้ใช้งานแอปพลิเคชันและระบบปฏิบัติการจึงควรเสริมความมั่นคงปลอดภัยของแอปพลิเคชันและระบบปฏิบัติการที่ใช้งานในสภาพแวดล้อมการให้บริการจริง เพื่อลดความเสี่ยงและความเสียหายที่อาจเกิดขึ้นจากการถูกโจมตีทางไซเบอร์ ซึ่งการเสริมสร้างความมั่นคงปลอดภัยของระบบ (System Hardening) หมายถึง กระบวนการในการลดพื้นที่การโจมตี (Attack surface) หรือพื้นที่ช่องโหว่ (Vulnerability Surface) และเส้นทางการโจมตีที่อาจเกิดขึ้นอื่น ๆ โดยการแพทช์ช่องโหว่ความมั่นคงปลอดภัยและปิดใช้งานบริการที่ไม่จำเป็น เอกสารฉบับนี้นำเสนอแนวปฏิบัติการเสริมความมั่นคงปลอดภัยแอปพลิเคชันและระบบปฏิบัติการเบื้องต้นเพื่อให้ผู้พัฒนาและผู้ใช้งานทราบถึงแนวปฏิบัติที่ดีพื้นฐานเพื่อยกระดับความมั่นคงปลอดภัยของระบบและหน่วยงาน

9.6.1. แนวทางและแนวปฏิบัติที่ดีการเสริมสร้างความมั่นคงปลอดภัยแอปพลิเคชัน

การเสริมสร้างความมั่นคงปลอดภัยแอปพลิเคชัน (Application hardening) เป็นการทำให้แอปพลิเคชันมีความมั่นคงปลอดภัยเพิ่มขึ้นโดยใช้กระบวนการต่าง ๆ รวมถึง การปรับปรุงให้ทันสมัย

(Updating) และการใช้มาตรการควบคุมอื่น ๆ เพิ่มเติมเพื่อปกป้องแอปพลิเคชันที่ติดตั้งมาพร้อมกับระบบปฏิบัติการและแอปพลิเคชันที่พัฒนาโดยผู้พัฒนาภายนอกและติดตั้งเพิ่มเติมในภายหลัง

การเสริมสร้างความมั่นคงปลอดภัยแอปพลิเคชันควรมีการดำเนินการในทุกขั้นตอนของการพัฒนา ตั้งแต่การออกแบบ การพัฒนา และการติดตั้งใช้งาน การเสริมสร้างความมั่นคงปลอดภัยตลอดวงจรชีวิตการพัฒนาแอปพลิเคชันมีแนวทางพื้นฐาน ดังนี้

1) มีการอ้างอิงมาตรฐานและใช้เครื่องมือความมั่นคงปลอดภัยในขั้นตอนการออกแบบและพัฒนาแอปพลิเคชัน เช่น การตรวจสอบช่องโหว่ความมั่นคงปลอดภัยของโค้ดที่พัฒนา เริ่มตั้งแต่ช่วงต้นของการพัฒนาแอปพลิเคชัน

2) มีการใช้กระบวนการและระบบความมั่นคงปลอดภัยเพื่อปกป้องแอปพลิเคชันที่อยู่สภาพแวดล้อมการใช้งานจริง เช่น การทดสอบความมั่นคงปลอดภัยอย่างสม่ำเสมอ

3) ใช้งานการพิสูจน์ตัวจริงที่เข้มงวด (Strong authentication) โดยเฉพาะกับแอปพลิเคชันที่มีการประมวลผลข้อมูลละเอียดอ่อนหรือมีความสำคัญต่อการให้บริการ ควรพิจารณาใช้งานการพิสูจน์ตัวจริงแบบหลายปัจจัย (Multi-factor authentication) เพื่อปกป้องการเข้าถึงระบบและข้อมูลที่สำคัญ

4) ใช้ระบบ และมาตรการรักษาความมั่นคงปลอดภัยเพิ่มเติม เพื่อปกป้องแอปพลิเคชัน เช่น Web Application Firewall (WAF) และ Intrusion Prevention System (IPS)

การเสริมสร้างความมั่นคงปลอดภัยแอปพลิเคชันในเชิงเทคนิค มีด้านต่าง ๆ ที่ควรจะต้องคำนึง ดังต่อไปนี้

1) การจัดการและการบันทึกข้อผิดพลาด ควรมีการจัดการและบันทึกข้อผิดพลาดไว้อย่างเหมาะสม โดยข้อความข้อผิดพลาดที่แสดงให้ผู้ใช้ทั่วไปเห็นไม่ควรมีข้อมูลรายละเอียดสถานะภายในของแอปพลิเคชัน มีการจัดการข้อผิดพลาดในทุกกรณีและควบคุมผลลัพธ์ที่แสดงให้กับผู้ใช้ หลีกเลี่ยงการแสดงข้อผิดพลาดตามการตั้งค่าเริ่มต้นของเฟรมเวิร์คที่ใช้ในการพัฒนา ปรับเปลี่ยนให้เป็นการแสดงข้อผิดพลาดที่มีการปรับแต่งแล้ว มีการเก็บบันทึกกิจกรรมการพิสูจน์ตัวจริง การเปลี่ยนแปลงระดับสิทธิการใช้งาน กิจกรรมที่ใช้สิทธิผู้ดูแลระบบ และการเข้าถึงข้อมูลสำคัญ ไม่ควรเก็บข้อมูลเกินจำเป็นในล็อก และเก็บข้อมูลอย่างมั่นคงปลอดภัย

2) การปกป้องข้อมูล หากเป็นแอปพลิเคชันที่มีการส่งต่อข้อมูลผ่านเครือข่าย ควรใช้การเชื่อมต่อที่มีความมั่นคงปลอดภัย เช่น HTTPS หรือ TLS หากมีการจัดการและเก็บรหัสผ่านผู้ใช้ควรปฏิบัติตามแนวปฏิบัติที่ดี เช่น ใช้อัลกอริทึมที่ออกแบบเพื่อใช้จัดเก็บรหัสผ่าน (เช่น PBKDF2 และ bcrypt) ร่วมกับการใช้ข้อมูลสุ่ม (salt)[8] เพื่อเพิ่มความปลอดภัย หากมีการใช้กุญแจรหัสลับ ควรมีการจัดการที่เหมาะสม ตั้งแต่การสร้าง การกระจาย การจัดเก็บ และการใช้งาน มีการเก็บข้อมูลโดยเฉพาะข้อมูลที่มีความละเอียดอ่อนเท่าที่จำเป็น เป็นระยะเวลาที่เหมาะสม และมีการทำลายข้อมูลนั้นเมื่อเลิกใช้งานแล้ว

[8] บางฟังก์ชันมีการใช้ salf เป็นค่าเริ่มต้นแล้ว ไม่ต้องทำกระบวนการอื่นเพิ่มเติม

3) การกำหนดค่าและการดำเนินการ พิจารณาการใช้ระบบการติดตั้งแอปพลิเคชันอัตโนมัติ (Automate application deployment) โดยเฉพาะ Continuous Integration and Continuous Deployment (CI/CD) เพื่อให้มั่นใจว่าการเปลี่ยนแปลงต่อแอปพลิเคชันมีความสอดคล้องและสามารถทำซ้ำได้ในทุกสภาพแวดล้อมมีการพัฒนากระบวนการจัดการการเปลี่ยนแปลงที่เข้มงวด มีการกำหนดความต้องการด้านความมั่นคงปลอดภัย มีการทบทวนการออกแบบ โค้ด และการตั้งค่า มีการวางแผนการรับมือเหตุการณ์ไม่คาดคิด

4) การพิสูจน์ตัวจริง ไม่เก็บข้อมูลการพิสูจน์ตัวจริง (Credential) ไว้ในโค้ดของแอปพลิเคชัน มีระบบการตั้งรหัสผ่านใหม่ที่รัดกุม มีการพัฒนานโยบายการใช้รหัสผ่านที่มั่นคงปลอดภัย พิจารณาเปลี่ยนไปใช้การพิสูจน์ตัวจริงแบบไม่ใช้รหัสผ่าน (เช่น FIDO2) มีการตั้งการล็อคบัญชีเมื่อใส่รหัสผ่านผิดจำนวนหนึ่งเพื่อทำให้การโจมตีแบบ Brute force ยากขึ้น การให้สิทธิกับผู้ใช้งานควรให้เท่าที่จำเป็นต่อการปฏิบัติงานของผู้ใช้แต่ละรายเท่านั้น สำหรับระบบที่มีความสำคัญหรือระบบที่มีการจัดเก็บหรือประมวลผลข้อมูลที่มีความละเอียดอ่อน ควรพิจารณาการพิสูจน์ตัวจริงแบบหลายปัจจัย กล่าวคือ เลือกใช้ปัจจัยสิ่งที่ผู้ใช้รู้ สิ่งที่ผู้ใช้มี หรือสิ่งที่ผู้ใช้เป็น ตั้งแต่สองปัจจัยเป็นต้นไป

5) การจัดการเซสชัน โทเคนเซสชันควรมีความสุ่มและความยาวที่เพียงพอต่อการวิเคราะห์และคาดเดา มีการสร้างโทเคนเซสชันใหม่เมื่อมีการลงชื่อเข้าใช้งานใหม่และเมื่อมีการเปลี่ยนแปลงระดับสิทธิการใช้งาน มีการตั้งค่าการลงชื่อออกอัตโนมัติเมื่อไม่ใช้งานเป็นระยะเวลาหนึ่งและมีการตั้งค่าลงชื่อออกจากระบบอัตโนมัติหลังจากลงชื่อเข้าใช้งานแล้วเป็นระยะเวลาหนึ่งเพื่อลดความเสี่ยงการถูกขโมยใช้เซสชัน ยกเลิกเซสชันเมื่อมีการลงชื่อออก มีเมนูให้ลงชื่อออกจากแอปพลิเคชันได้สะดวก

6) การจัดการข้อมูลนำเข้าและข้อมูลส่งออก มีการเข้ารหัสข้อมูลผลลัพธ์ตามบริบทที่เหมาะสม เช่น ข้อมูลในบริบท URL และข้อมูลในบริบท JavaScript ถ้าเป็นไปได้เลือกใช้ Allow list หรือ White list แทน Block list หรือ Black list สำหรับข้อมูลนำเข้า ใช้การส่งข้อมูลค้นหา SQL แบบพารามิเตอร์แทนการใช้สตริง ใช้โทเคนเพื่อป้องการการปลอมแปลงคำร้องขอ มีการตั้งค่ารหัสอักษร (Encoding) อย่างเหมาะสม มีการตรวจสอบข้อมูลที่นำเข้าจากภายนอกเสมอโดยทำที่ฝั่งเซิร์ฟเวอร์ด้วย ไม่ใช่เฉพาะที่ฝั่งไคลเอนท์ มีการถอดรหัสข้อมูลที่อาจมาจากแหล่งไม่น่าเชื่อถือด้วยการควบคุมความมั่นคงปลอดภัยที่เหมาะสม

7) การควบคุมการเข้าถึง มีการใช้การควบคุมการเข้าถึงตามจุดต่าง ๆ ของระบบอย่างเหมาะสม ใช้หลักการสิทธิพิเศษที่น้อยที่สุดในการปฏิบัติงาน (the Principle of least privilege)

นอกจากนี้ เนื่องจากแอปพลิเคชันส่วนใหญ่ โดยเฉพาะแอปพลิเคชันที่มีการเชื่อมต่อข้อมูลออนไลน์ และรวมถึงแอปพลิเคชันที่ทำงานแบบออฟไลน์ มักมีการเชื่อมต่อกับบริการหรือแอปพลิเคชันอื่น ๆ เพื่อแลกเปลี่ยนข้อมูลและดำเนินการฟังก์ชันที่มีความหลากหลายเพื่ออำนวนความสะดวกและทำงานตามที่ผู้ใช้ต้องการ การรักษาความมั่นคงปลอดภัยสำหรับช่องทางการเชื่อมต่อแลกเปลี่ยนข้อมูล หรือ ส่วนต่อประสานโปรแกรมประยุกต์ (Application Programming Interface [API]) สามารถศึกษาได้จาก “แนวปฏิบัติการรักษาความมั่นคงปลอดภัย API”

9.6.2. แนวทางและแนวปฏิบัติที่ดีการเสริมสร้างความมั่นคงปลอดภัยระบบปฏิบัติการ

การเสริมสร้างความมั่นคงปลอดภัยระบบปฏิบัติการ (Operating system hardening) มีการติดตั้งแพทช์และใช้มาตรการความมั่นคงปลอดภัยขั้นสูงในการปกป้องระบบปฏิบัติการ การเสริมสร้างความมั่นคงปลอดภัยของระบบปฏิบัติการมีความคล้ายคลึงกับการเสริมสร้างความมั่นคงปลอดภัยแอปพลิเคชันเพราะต่างก็เป็นซอฟท์แวร์เหมือนกัน แต่มีความต่างที่การเสริมสร้างความมั่นคงปลอดภัยระบบปฏิบัติการเน้นการปกป้องซอฟท์แวร์ที่เป็นส่วนพื้นฐานในการประสานและให้บริการกับแอปพลิเคชันต่าง ๆ

ถึงแม้ว่าระบบปฏิบัติการต่าง ๆ จะมีลักษณะที่แตกต่างกันออกไป มีแนวทางการเสริมสร้างความปลอดภัยบางอย่างที่สามารถประยุกต์ใช้ได้กับระบบปฏิบัติการเหล่านี้ ได้แก่

1) การปรับปรุงระบบปฏิบัติให้เป็นปัจจุบันอยู่เสมอ ถึงแม้ว่าการปรับปรุงระบบให้เป็นปัจจุบันจะไม่สามารถปกป้องต่อภัยคุกคามได้ทุกอย่าง แต่ก็สามารถลดความเสี่ยงที่อาจถูกโจมตีลงได้เป็นอย่างมาก

2) การจัดการแพทช์ รวมถึงการวางแผน การทดสอบ การติดตั้งอย่างทันเวลา และการตรวจสอบอย่างสม่ำเสมอ เพื่อให้ระบบได้ติดตั้งแพทช์ที่เป็นปัจจุบันและไม่กระทบต่อการทำงานของระบบเดิม

3) ลบแอปพลิเคชันและบริการที่ไม่มีความจำเป็นต่อการใช้งาน รวมถึงการตรวจสอบและถอนการติดตั้งแอปพลิเคชันและบริการที่ไม่ได้ใช้งาน ซึ่งควรทำอย่างสม่ำเสมอ เพื่อลดพื้นที่ในการโจมตีเพราะซอฟท์แวร์เหล่านี้อาจมีช่องโหว่ความมั่นคงปลอดภัยอยู่

4) เปิดใช้งานเฉพาะพอร์ตและบริการที่ต้องใช้งาน ควรปิดพอร์ตที่ไม่ใช้งานเพราะพอร์ตเหล่านี้อาจถูกใช้เป็นช่องทางในการโจมตีโดยผู้ไม่ประสงค์ดี และควรปิดบริการที่ไม่ได้ใช้งานด้วย

5) ถอนการติดตั้งไดร์เวอร์อุปกรณ์ที่ไม่จำเป็น รวมถึงการระบุไดร์เวอร์เก่าหรือไม่ได้ใช้งานและถอนการติดตั้ง เนื่องจากไดร์เวอร์เหล่านี้อาจมีช่องโหว่ความมั่นคงปลอดภัยที่ไม่ได้รับการติดตั้งแพทช์และอาจถูกใช้โดยผู้ไม่ประสงค์ดีในการเข้าสู่ระบบโดยไม่ได้รับอนุญาตได้

6) มีใช้กฎการเข้าถึงที่เข้มงวด ใช้ความสามารถของระบบในการควบคุมการเข้าถึงไฟล์ เครือข่าย และทรัพยากรอื่น ๆ ค่าเริ่มต้นของระบบปฏิบัติการมักจะเข้มงวดน้อยกว่าที่ควรจะเป็น จึงควรมีการตั้งค่าให้เหมาะสม โดยยึดหลักสิทธิพิเศษที่น้อยที่สุด ให้สิทธิเฉพาะผู้ที่ต้องการใช้ และเมื่อจำเป็นต้องใช้เท่านั้น

7) จำกัดการสร้างบัญชีผู้ใช้และมีการตรวจสอบบัญชีผู้ใช้อย่างสม่ำเสมอ สร้างเฉพาะบัญชีผู้ใช้ที่จำเป็นต่อการใช้งานของผู้ใช้เท่านั้น ปิดการใช้งานของบัญชีชั่วคราวเมื่อเลิกใช้งาน ตรวจสอบและทบทวนสิทธิหรือปิดบัญชีของผู้ใช้งานที่มีการย้ายแผนกหรือออกจากงาน โดยตรวจสอบและทบทวนอย่างสม่ำเสมอ

8) ตั้งนโยบายกรุ๊ปอย่างเหมาะสม โดยจัดกลุ่มบัญชีผู้ใช้ที่มีสิทธิการใช้งานเหมือนกันเป็นกรุ๊ปและตั้งค่าการเข้าถึงอย่างเข้มงวดตามที่จำเป็นเพื่อลดความเสียหายในกรณีที่บัญชีถูกผู้ไม่ประสงค์ดีเข้าใช้งาน

9) มีการทำเทมเพลตความมั่นคงปลอดภัย ใช้เทมเพลตในการจัดการและบังคับใช้การกำหนดค่าความมั่นคงปลอดภัยแบบรวมศูนย์ เพื่อช่วยให้การจัดการการตั้งค่าต่าง ๆ มีความสอดคล้องกันทั้งหน่วยงาน

10) ใช้เฟรมเวิร์กเสริมสร้างความมั่นคงปลอดภัย สำหรับระบบปฏิบัติการ Linux สามารถใช้ AppArmor และ SELinux เพื่อยกระดับการควบคุมการเข้าถึงและปกป้องจากการโจมตี เช่น buffer overflow และ code injection เฟรมเวิร์กเหล่านี้สามารถช่วยติดตั้งและใช้งานการตั้งค่าตามแนวปฏิบัติที่ดีทั่วไปได้ในระดับหนึ่งโดยอัตโนมัติ

11) แบ่งแยกข้อมูลและการทำงาน แอปพลิเคชันและข้อมูลที่มีความละเอียดอ่อนควรแยกอยู่ในสภาพแวดล้อมที่แยกออกจากแอปพลิเคชันและข้อมูลอื่น ๆ เพื่อลดความเสี่ยงในการถูกโจมตีและจำกัดของเขตความเสียหาย

12) เข้ารหัสลับหน่วยเก็บข้อมูลที่มีการจัดเก็บข้อมูลที่มีความละเอียดอ่อน เพื่อป้องการการเข้าถึงโดยไม่ได้รับอนุญาตถึงแม้ว่าผู้ไม่ประสงค์ดีจะสามารถเข้าถึงหน่วยเก็บข้อมูลด้วยวิธีการทางกายภาพได้

13) ใช้งานระบบรักษาความมั่นคงปลอดภัยเพิ่มเติม เช่น Firewall, Intrusion Protection System, Endpoint protection

14) ผู้ใช้งานแต่ละรายควรมีบัญชีผู้ใช้แยกเป็นของตนเอง รวมถึงกรณีที่ผู้ใช้งานหลายคนใช้งานคอมพิวเตอร์เครื่องเดียวกัน การพิสูจน์ตัวจริงควรเลือกปัจจัยในการพิสูจน์ตัวจริงที่เหมาะสม สำหรับบัญชีผู้ดูแลระบบหรือบัญชีที่มีสิทธิการใช้งานสูง ควรมีการพิจารณาใช้งานการพิสูจน์ตัวจริงแบบหลายปัจจัยเพื่อลดความเสี่ยงจากการที่ผู้ไม่ประสงค์ดีเข้าใช้งานบัญชีโดยไม่ได้รับอนุญาต

สำหรับผู้ที่สนใจรายละเอียดเกี่ยวกับแนวปฏิบัติที่ดีในการเสริมสร้างความมั่นคงปลอดภัยแอปพลิเคชันและระบบปฏิบัติการ สามารถศึกษาข้อมูลเพิ่มเติมได้จากแหล่งข้อมูลและเอกสารดังต่อไปนี้

- OS Hardening: 15 Best Practices, Perception Point, https://perception-point.io/guides/os-isolation/os-hardening-10-best-practices/
- Securing Web Application Technologies [SWAT] Checklist, SANS, https://www.sans.org/cloud-security/securing-web-application-technologies/
- Essential Eight user application hardening, Microsoft, https://learn.microsoft.com/en-us/compliance/essential-eight/e8-app-harden
- What is System Hardening? Essential Checklists from OS to Applications, Canonical Ubuntu, https://ubuntu.com/blog/what-is-system-hardening-definition-and-best-practices
- Guide to General Server Security (NIST SP 800-123), NIST, https://www.nist.gov/publications/guide-general-server-security

– Keeping Information Technology (IT) System Servers Secure: A General Guide to Good Practices, NIST, https://www.nist.gov/publications/keeping-information-technology-it-system-servers-secure-general-guide-good-practices

– CISecurity, https://www.cisecurity.org/

10. ข้อแนะนำเพิ่มเติมสำหรับผู้ใช้งานทั่วไปในชีวิตประจำวัน

ความปลอดภัยในโลกไซเบอร์ (Cyber Safety) ไม่ใช่แค่เรื่องไกลตัวอีกต่อไปในชีวิตประจำวันของเราล้วนเกี่ยวข้องกับโลกไซเบอร์ หรือโลกออนไลน์ ตั้งแต่การใช้โทรศัพท์มือถือ ใช้สื่อสังคมออนไลน์ ซื้อของออนไลน์ ทำธุรกรรมการเงินออนไลน์ หรือแม้แต่การติดต่อประสานงานผ่านช่องทางออนไลน์ ความปลอดภัยไซเบอร์จึงมีความสำคัญยิ่ง โดยเฉพาะการปกป้องข้อมูลส่วนตัว การลดความเสี่ยงโดนหลอกลวง โจรกรรม การระรานทางไซเบอร์ (Cyberbullying) หรือข้อมูลรั่วไหล เราสามารถเริ่มต้นง่าย ๆ ด้วยแนวทางที่ปลอดภัย เช่น การตั้งรหัสผ่านที่ปลอดภัย การไม่แชร์ข้อมูลสำคัญไปยังสาธารณะ การเลือกใช้บริการออนไลน์ที่น่าเชื่อถือ การเลือกซื้อสินค้าจากแหล่งปลอดภัย การหมั่นอัพเดตอุปกรณ์ การฝึกนิสัยสำรองข้อมูล และการระมัดระวังในการใช้สื่อสังคมออนไลน์ เป็นต้น ในบทนี้ จะแนะนำการสร้างเกราะป้องกันให้ผู้ใช้งานรู้สึกปลอดภัยไร้กังวลและเผชิญโลกออนไลน์อย่างมั่นใจ

10.1. การใช้อุปกรณ์พกพาอย่างปลอดภัย (Mobile Device Safety)

ปัจจุบัน อุปกรณ์อิเล็กทรอนิกส์แบบพกพามีการพัฒนาออกมาในหลาย ๆ รูปแบบ ไม่ว่าจะเป็นโทรศัพท์มือ แท็บเล็ต สมาร์ทวอทช์ หรืออุปกรณ์อิเล็กทรอนิกส์ในรูปแบบอื่น ๆ อย่างอุปกรณ์อินเทอร์เน็ตของสรรพสิ่ง (Internet of Things: IoT) เช่นกล้องวงจรปิดอัจฉริยะ หรืออุปกรณ์สมาร์ทโฮม เป็นต้น ซึ่งอุปกรณ์เหล่านี้ทำหน้าที่เหมือนคอมพิวเตอร์เครื่องหนึ่ง หรืออุปกรณ์สื่อสารที่มีขนาดเล็กที่พกพา สวมใส่ หรือนำไปติดตั้งในที่ใด ๆ ก็ได้ ดังนั้นอุปกรณ์เหล่านี้จึงสามารถจัดเก็บข้อมูล และรับส่งข้อมูลผ่านเครือข่ายคอมพิวเตอร์เฉกเช่นคอมพิวเตอร์เครื่องหนึ่ง ซึ่งมีความเสี่ยงที่ข้อมูลเหล่านี้สามารถถูกขโมย โจมตี หรือโจรกรรมได้ง่าย เนื่องจากอยู่ในอุปกรณ์ขนาดเล็กที่สามารถพกพาไปที่ใดก็ได้ ดังนั้นผู้ใช้งานจึงควรใช้งานอุปกรณ์พกพาเหล่านี้ด้วยวิธีแบบปลอดภัย

ขั้นตอนปฏิบัติ

1. ตั้งรหัสผ่านที่ยากต่อการคาดเดาในการเข้าถึงอุปกรณ์พกพา ในกรณีที่อุปกรณ์ถูกขโมยหรือสูญหาย ผู้อื่นจะไม่สามารถเข้าถึงข้อมูลอุปกรณ์เพื่อใช้งานได้
2. ควรเชื่อมต่อเครือข่ายที่เชื่อถือได้เท่านั้น เช่น ระบบเครือข่ายของหน่วยงาน หรือระบบเครือข่ายของผู้ให้บริการที่เชื่อถือได้ ไม่ควรเชื่อมต่อเครือข่าย Wi-Fi ที่ไม่รู้จัก โดยเฉพาะอย่างยิ่งเมื่อต้องการรับส่งข้อมูลที่เป็นความลับ เพื่อหลีกเลี่ยงการถูกขโมยข้อมูล
3. ควรอัพเดตระบบปฏิบัติการ หรือโปรแกรม หรือแอปฯ ที่มีการอัพเดต Patch อย่างสม่ำเสมอ
4. ติดตั้งโปรแกรมสแกนไวรัสที่น่าเชื่อถือ
5. ระมัดระวังเมื่อดาวน์โหลดแอปฯ ทุกครั้ง และควรดาวน์โหลดจากแหล่งที่เป็นทางการ เช่น Play Store หรือ App Store
6. ควรติดตั้งโปรแกรมเพื่อติดตามหาอุปกรณ์เมื่อสูญหาย ในกรณีที่อุปกรณ์ถูกขโมยหรือสูญหาย เจ้าของจะสามารถรู้ตำแหน่งของอุปกรณ์นั้นได้

7. ควรเลือกการยืนยันตัวตนแบบสองปัจจัยขึ้นไป (Two-Factor Authentication) สำหรับการลงชื่อเข้าใช้งานระบบที่ผู้ใช้งานต้องการความปลอดภัยสูง

8. เข้ารหัสข้อมูลในอุปกรณ์ สำหรับข้อมูลที่เป็นความลับ หรือมีความอ่อนไหว

9. ระมัดระวังในการกดลิงค์ (Link) หรืออีเมลที่น่าสงสัย ซึ่งอาจเป็นการโจมตีแบบฟิชชิง (Phishing) ที่หลอกขโมยข้อมูลของผู้ใช้งาน หรือมีการแฝงโปรแกรมประเภทมัลแวร์ที่โจมตีข้อมูลในอุปกรณ์

10. ทำการสำรองข้อมูลในอุปกรณ์อย่างสม่ำเสมอ

11. ไม่ควรแชร์ข้อมูลส่วนบุคคล ไม่ว่าจะเป็นที่อยู่ หรือเบอร์โทรศัพท์ ผู้ไม่ประสงค์ดีสามารถสแกนหาข้อมูลดังกล่าวเพื่อติดตามการใช้ชีวิตของเหยื่อได้

12. ปิดการใช้งานฟังก์ชันการระบุตำแหน่งถ้าไม่จำเป็น เช่น ฟังก์ชันการระบุตำแหน่งเมื่อถ่ายรูป (Photo Geotagging) ถ้าฟังก์ชันการระบุตำแหน่งนี้ถูกเปิดไว้ เมื่อมีการถ่ายรูป ข้อมูลตำแหน่งจะถูกจัดเก็บเป็นเมตาเดต้า (Metadata) ของรูปภาพนั้น และเมื่อแชร์รูปภาพดังกล่าวออกไป ผู้ไม่ประสงค์ดีก็จะสามารถรู้ที่อยู่ขณะที่ถ่ายภาพทันที ซึ่งอาจเป็นอันตรายต่อบุคคลที่อยู่ในภาพโดยเฉพาะเด็ก และเยาวชน คำแนะนำนี้รวมถึงการจงใจแชร์ที่อยู่เมื่อมีการโพสต์ข้อมูลใด ๆ ลงสื่อสังคมออนไลน์ด้วย

13. หากหน่วยงานซื้ออุปกรณ์เหล่านี้เพื่อใช้ในสำนักงาน ควรที่จะติดตั้งโปรแกรมที่สามารถควบคุมการใช้งานก่อน เพื่อไม่ให้ผู้ใช้งานนำไปใช้ผิดวัตถุประสงค์ หรืออย่างน้อยผู้ดูแลระบบสามารถตรวจสอบการใช้งานได้

14. สำหรับอุปกรณ์ประเภท IoT หรือสมาร์ทโฮม ผู้ใช้งานต้องเปลี่ยนรหัสผ่านตั้งต้น (Default Password) ของอุปกรณ์ โดยทั่วไปอุปกรณ์เหล่านี้จะถูกตั้งค่าเริ่มต้นมาตั้งแต่ที่โรงงานผลิต และค่ารหัสผ่านตั้งต้นนี้มักจะเหมือนกันทุกเครื่องที่มียี่ห้อ และรุ่นเดียวกัน ซึ่งแฮกเกอร์สามารถเลือกใช้รหัสผ่านตั้งต้นของยี่ห้อหรือรุ่นนั้นในการเข้าถึงอุปกรณ์ที่เป็นเป้าหมาย ดังนั้น เมื่อผู้ใช้งานซื้ออุปกรณ์มา ควรจะเปลี่ยนรหัสผ่านทันที

15. หน่วยงานควรมีการจัดฝึกอบรมความตระหนักในการใช้อุปกรณ์พกพาอย่างปลอดภัยอย่างสม่ำเสมอ

10.2. การรักษาความเป็นส่วนตัว (Privacy Protection)

การรักษาความเป็นส่วนตัวในโลกออนไลน์ รวมถึงการคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องที่สำคัญซึ่งไม่สามารถแยกขาดจากกันกับเรื่องความมั่นคงปลอดภัยไซเบอร์ได้ ผู้ใช้งานทุกคนจะต้องเข้าใจแนวคิดเรื่องความเป็นส่วนตัว และการคุ้มครองข้อมูลส่วนบุคคลว่ามีความสำคัญต่อตนเอง และผู้อื่นเพียงใด การรักษาความเป็นส่วนตัว และการคุ้มครองข้อมูลส่วนบุคคลนั้น จะต้องรวมทั้งข้อมูลของตนเอง และของผู้อื่นด้วย การปล่อยให้มีการรุกล้ำความเป็นส่วนตัว หรือการที่ข้อมูลส่วนบุคคลถูกเปิดเผยออกไปเกินความจำเป็นนั้นจะเกิดผลกระทบหลายอย่าง เช่น เกิดความรำคาญ อับอาย กีดกัน หรือปัญหาด้านความปลอดภัยในชีวิตและทรัพย์สิน และยังรวมถึงผลกระทบทางกฎหมายอีกด้วย นอกจากนี้ ยังจำเป็นต้องรู้ถึงแนวทางในการปฏิบัติเพื่อลดความเสี่ยงต่อความเสียดายดังกล่าวด้วย ซึ่งจะได้สอดคล้องกับมาตรการทางกฎหมายที่เกี่ยวข้องกับการรักษาความเป็นส่วนตัว และการคุ้มครองข้อมูลส่วนบุคคล

ขั้นตอนปฏิบัติ

1. ไม่เปิดเผยข้อมูลส่วนบุคคลเกินความจำเป็น ไม่ว่าจะเป็นของตนเอง หรือผู้อื่นที่อาจก่อให้เกิดความเสียหายต่อตนเอง หรือผู้อื่นตามมา เช่น การเปิดเผยที่อยู่บ้าน โทรศัพท์มือถือ เลขบัตรประชาชนลงสื่อสังคมออนไลน์ การเปิดเผยข้อมูลสุขภาพของผู้ป่วยในที่สาธารณะ การแท็ก (Tag) บุคคลอื่นโดยไม่ได้รับอนุญาตโดยที่บุคคลนั้นอาจไม่ต้องการให้แท็ก การโพสต์ภาพเพื่อนที่อยู่ในท่าทางที่น่าอับอาย เป็นต้น

2. ผู้ใช้งานควรตั้งค่าความเป็นส่วนตัวในโปรแกรมเพื่อปกป้องตนเอง เช่น การตั้งค่าให้มีการแจ้งเตือนเมื่อถูกแท็ก การตั้งค่าไม่ให้เปิดเผยวันเกิด การตั้งค่าไม่ให้ค้นหาชื่อตนเอง เป็นต้น รวมถึงการเลือกใช้ฟังก์ชันที่ปกป้องความเป็นส่วนตัวชั้นสูง เช่น การเลือกใช้ Incognito Mode ในเว็บบราวเซอร์ การปิดฟังก์ชันการติดตามสถานที่ (Location Tracking) เป็นต้น

3. ให้ความรู้เรื่องการรักษาความเป็นส่วนตัวในโลกออนไลน์ รวมถึงการคุ้มครองข้อมูลส่วนบุคคล ตั้งแต่วัยเด็ก หรือโดยเร็ว เพื่อปรับทัศนคติ และเสริมสร้างวัฒนธรรมที่ดีตั้งแต่วัยเยาว์

4. ตั้งค่ารหัสผ่านให้ยากต่อการคาดเดา หรือใช้การยืนยันแบบสองปัจจัย (Two-Factor Authentication) เพื่อลดความเสี่ยงที่ผู้อื่นที่จะขโมยข้อมูลในระบบ

5. ควรแชร์ข้อมูลเท่าที่จำเป็น (Need-to-Know Basis) ไม่จำเป็นจะต้องแชร์ข้อมูลไปหมดเสียทุกอย่าง

6. เมื่อจำเป็นต้องแชร์ข้อมูลให้ผู้อื่น ควรตรวจสอบเสียก่อนว่ามีข้อมูลส่วนบุคคลอยู่ในนั้นหรือไม่ ถ้ามี และไม่จำเป็นต้องแชร์ข้อมูลส่วนบุคคลนั้น ต้องลบข้อมูลส่วนบุคคลออกเสียก่อน หรือใช้กรรมวิธีในการแปลงข้อมูลนั้นให้เป็นนิรนาม (Anonymization) ที่ไม่สามารถระบุตัวตนได้

7. เมื่อเกิดปัญหาร้องเรียนจากการเปิดเผย หรือแชร์ข้อมูลส่วนบุคคลที่ส่งผลกระทบกับผู้อื่นโดยตรง ควรที่จะนำข้อมูลนั้นออกทันทีก่อน และหาแนวทางการแก้ปัญหาต่อไป เช่น ผู้ใช้งานแชร์ภาพตนเองที่ติดกับภาพผู้อื่น และบุคคลในภาพได้ขอให้นำออก ผู้ใช้งานควรที่จะนำภาพนั้นออกทันที และพิจารณาว่าควรจะทำอย่างไรต่อไป ไม่ว่าจะเป็นการเลือกที่จะเบลอหน้าบุคคลนั้นแล้วแชร์ใหม่อีกครั้ง หรือไม่ต้องดำเนินการใด ๆ อีก

8. เมื่อต้องนำอุปกรณ์ไปให้ผู้อื่น เช่น การส่งซ่อม ผู้ใช้งานต้องตรวจสอบว่ายังคงมีข้อมูลส่วนบุคคล หรือข้อมูลที่เป็นความลับ ที่ผู้อื่นสามารถเข้าถึงโดยง่าย หลงเหลืออยู่ หรือไม่ ถ้ายังมี จะต้องหาวิธีที่เหมาะสมในการป้องกันการเข้าถึง เช่น การลบข้อมูล และสำรองข้อมูลไว้ที่แหล่งอื่น การเข้ารหัส หรือใช้ระบบควบคุมการเข้าถึงอื่น ๆ เป็นต้น

9. เมื่อไม่ใช้อุปกรณ์นั้นอีกต่อไป ต้องทำลายข้อมูลในอุปกรณ์นั้นด้วยวิธีที่สามารถทำได้ด้วยตนเองอย่างเหมาะสม เช่น การฟอร์แมต (Format) การล้างเครื่องโทรศัพท์ (Factory Reset) การบดละเอียด เป็นต้น

10. ศึกษากฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

11. ศึกษาแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ควบคู่กันไปด้วย

10.3. การซื้อของ และการทำธุรกรรมทางธนาคารออนไลน์อย่างปลอดภัย (Safe Shopping and Banking)

การทำธุรกรรมออนไลน์ ไม่ว่าจะเป็นการซื้อของ หรือการทำธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์ต่าง ๆ ยังคงมีความเสี่ยงที่จะถูกหลอก หรือสูญเสียทรัพย์สินเสมอ ผู้ใช้งานไม่ควรที่จะเร่งรีบในการทำธุรกรรมจนเกินไป แต่การคิด วิเคราะห์ และดำเนินการอย่างระมัดระวังจะช่วยป้องกันไม่ให้ผู้ใช้งานสูญเสียเงิน หรือถูกขโมยข้อมูลสำคัญอื่น ๆ เช่น หมายเลขบัตรเครดิต บัญชีรายชื่อ และรหัสผ่าน เป็นต้น ผู้ใช้งานควรที่จะสละเวลาเล็กน้อยในการตรวจสอบองค์ประกอบต่าง ๆ ก่อนที่จะเริ่มทำธุรกรรมใด ๆ เพื่อไม่ให้เกิดความสูญเสียทรัพย์สินในระยะยาว

ขั้นตอนปฏิบัติ

1. **เว็บไซต์** ในการซื้อของออนไลน์ หรือทำธุรกรรมการเงินผ่านเว็บไซต์ ควรสังเกตว่า URL ของเว็บไซต์จะต้องขึ้นต้นด้วย “https://” (ไม่ใช่แค่ http) ตัว “s” หมายถึงว่าข้อมูลจะถูกเข้ารหัสในระหว่างการทำธุรกรรมออนไลน์ หากเว็บไซต์นั้น ไม่ใช้ https หมายความว่าข้อมูลในการทำธุรกรรมสามารถถูกดักขโมยได้
2. **บัตรเครดิต** ในการซื้อของออนไลน์ ควรใช้บัตรเครดิตมากกว่าบัตรเดบิต เนื่องจากการใช้บัตรเครดิตจะมีกลไกการปกป้องจากกลโกง (Fraud Prevention) มากกว่าบัตรเดบิต เช่น มีตัวกลางในการตรวจจับความผิดปกติของการจับจ่าย และผู้ใช้งานอาจได้รับการปกป้องไม่ต้องรับผิดชอบต่อความเสียหายจากการถูกโกง เป็นต้น นอกจากนี้ การใช้บัตรเดบิตซึ่งไม่มีตัวกลางนั้น ทำให้การทำธุรกรรมจะถูกเชื่อมไปยังบัญชีธนาคารของผู้ใช้งานโดยตรงทำให้มีความเสี่ยงมากกว่าการใช้บัตรเครดิต
3. **ตรวจสอบเว็บไซต์ก่อนเสมอ** เมื่อค้นหาข้อมูลสินค้าผ่านทาง Search Engine เช่น Google ควรตรวจสอบความถูกต้องของ URL ทุกครั้งว่าเป็นเว็บไซต์ที่ถูกต้อง หรือไม่ และในการเข้าถึงเว็บไซต์ควรที่จะพิมพ์ URL มากกว่าคลิกที่ URL นั้น ซึ่งการคลิกนั้นอาจจะนำพาไปยังเว็บไซต์ปลอม
4. **รหัสผ่าน** กำหนดรหัสผ่านให้ยากต่อการเดา ประกอบด้วยอักขระอย่างน้อย 8 ตัว และมีความซับซ้อน ใช้การยืนยันตัวตนสองปัจจัย (Two-Factor Authentication) เช่น รหัสผ่านร่วมกับ OTP ถ้าสามารถทำได้ และผู้ใช้งานต้องจำไว้ว่า จะต้องไม่มอบรหัสผ่านให้กับใคร ธนาคาร หรือร้านค้าไม่เคยที่จะร้องขอรหัสผ่านจากลูกค้า
5. **Wi-Fi** ไม่ใช้ Wi-Fi สาธารณะที่ฟรี หรือ Wi-Fi ที่ไม่น่าเชื่อถือสำหรับการซื้อของออนไลน์หรือทำธุรกรรมทางการเงิน เนื่องจากผู้ให้บริการ Wi-Fi นั้นอาจไม่มีมาตรการด้านการรักษาความปลอดภัยที่เพียงพอ
6. **ฟิชชิง (Phishing)** เมื่อได้ข้อความไม่ว่าจากอีเมล SMS หรือโปรแกรมต่าง ๆ เช่น LINE หรือ Facebook ควรพิจารณาถึงความน่าเชื่อถือว่าถูกส่งจากแหล่งที่มาที่ถูกต้อง หรือไม่ และต้องศึกษานโยบายของแหล่งที่มาว่ามีการส่งข้อมูลมาในลักษณะนี้ หรือไม่ เช่น ธนาคารจะไม่เคยขอข้อมูลส่วนบุคคลจากลูกค้าผ่านช่องทางอิเล็กทรอนิกส์ใด ๆ เป็นต้น หากจำเป็นต้องเข้าเว็บไซต์ดังกล่าวอยู่แล้ว ควรที่จะพิมพ์ URL ใหม่แทนการคลิก Link ที่ส่งมา

7. แอปฯ การใช้แอปฯ สำหรับการซื้อของ หรือทำธุรกรรมการเงินของธนาคาร ควรดาวน์โหลดจากแหล่งที่มาที่น่าเชื่อถือ เช่น App Store หรือ Play Store ไม่ใช่คลิก Link ที่เป็นไฟล์นามสกุล .apk และก่อนดาวน์โหลด ควรตรวจสอบข้อมูลอื่น ๆ ประกอบเช่น จำนวนการดาวน์โหลด รีวิว เจ้าของแอปฯ เป็นต้น

8. เครื่องคอมพิวเตอร์สาธารณะ หากใช้เครื่องคอมพิวเตอร์สาธารณะ อย่าลืม Log out ภายหลังจากการซื้อของออนไลน์ หรือทำธุรกรรมการเงินเสมอ

9. การโอนเงิน หากมีการโอนเงินผ่านแอปฯ ใด ๆ ต้องจำไว้เสมอว่าก่อนกดยืนยัน จะต้องตรวจสอบข้อมูลผู้รับโอน และจำนวนเงินเสมอว่าถูกต้อง หรือไม่ ไม่มีแอปฯ ใดที่เงินจะถูกโอนโดยอัตโนมัติที่ผู้ใช้งานยังไม่ได้ทำการยืนยัน

10. การร้องเรียน หากพบปัญหาการซื้อสินค้าออนไลน์ และต้องการคำปรึกษา สามารถแจ้งได้ที่ศูนย์รับเรื่องร้องเรียนปัญหาออนไลน์ (1212 Online Complaint Center หรือ 1212 OCC) ภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) https://1212etda.com/

10.4. การใช้สื่อสังคมออนไลน์อย่างปลอดภัย (Social Media Security)

การใช้สื่อสังคมออนไลน์ในปัจจุบันเป็นเรื่องที่มีความจำเป็นอย่างเลี่ยงไม่ได้ ไม่ว่าจะวัตถุประสงค์เพื่อใช้ติดต่อกับเพื่อนฝูง เพื่อประโยชน์ทางธุรกิจ หรือเพื่อเหตุผลใด ๆ ในฐานะผู้ใช้งาน ก่อนที่จะโพสต์ข้อความ หรือแสดงความเห็นใด ๆ จะต้องหยุด และคิดสักนิด ว่าข้อมูลที่จะโพสต์นั้นจะส่งผลกระทบอะไรบ้าง ต้องไม่โพสต์ข้อมูลส่วนบุคคล หรือข้อมูลที่อ่อนไหวไม่ว่าจะของตนเอง หรือผู้อื่น เพื่อลดความเสี่ยงต่อผลกระทบทั้งชีวิต ทรัพย์สิน และชื่อเสียง ซึ่งมีข้อปฏิบัติดังต่อไปนี้

ข้อควรปฏิบัติ

1. หยุด และคิดก่อนโพสต์ทุกครั้ง พิจารณาว่าสิ่งที่โพสต์จะส่งผลกระทบอะไรบ้าง
2. ข้อมูลที่โพสต์ ไม่ควรที่จะมีข้อมูลส่วนบุคคลทั้งของตนเอง และผู้อื่น หากเป็นรูปภาพจะต้องทำการลบส่วนที่เป็นข้อมูลส่วนบุคคลนั้นเสมอ เช่น หมายเลขบัตรประชาชน หมายเลขหนังสือเดินทาง เบอร์โทรศัพท์มือถือ ใบหน้าผู้อื่น (ในกรณีที่อาจทำให้ผู้อื่นได้รับความเสียหาย หรืออับอาย) ข้อมูลสุขภาพ เป็นต้น
3. ไม่ควรเปิดเผยข้อมูลมากเกินไป (Over-Sharing) โดยเฉพาะการแชร์กิจกรรมของตนเองในชีวิตประจำวันเกินความจำเป็น ซึ่งจะเป็นช่องทางให้ผู้ประสงค์ร้ายสามารถตามติดการดำเนินชีวิตได้
4. ก่อนแท็ก (Tag) บุคคลอื่น ควรขออนุญาตเจ้าตัวก่อน เพราะการ Tag บุคคลอื่น เสมือนเป็นการบอกว่าบุคคลนั้นอยู่กับผู้ใด ที่ใด เวลาใด ซึ่งถือเป็นข้อมูลส่วนบุคคล และเจ้าตัวอาจไม่ยินยอม
5. หากได้แชร์รูปภาพที่ติดบุคคลอื่น และเจ้าตัวได้ติดต่อขอให้ลบออก ควรพิจารณาลบออก หรือทำการเบลอใบหน้าบุคคลนั้น ไม่ว่าการแชร์รูปภาพนั้นจะผิด หรือไม่ผิดกฎหมายก็ตาม
6. ไม่ควรโพสต์ข้อมูล หรือแสดงความเห็น ในระหว่างที่อยู่อารมณ์โกรธ หรือไม่อยู่ในอารมณ์ที่สงบ

7. ควรตั้งค่าความเป็นส่วนตัว (Privacy) ให้มีความเหมาะสม เช่น ให้มีการแจ้งเตือนทุกครั้งที่ถูก Tag ใน Facebook หรือการตั้งค่าบัญชีให้ Private ใน Instagram เป็นต้น

8. ก่อนโพสต์ ควรเลือกรูปแบบการมองเห็นโดยบุคคลอื่นให้เหมาะสม เช่น เปิดสาธารณะ หรือเห็นกลุ่มเพื่อน เป็นต้น

9. เมื่อพบความผิดปกติจากเพจใด ๆ ในสื่อสังคมออนไลน์ ควรรายงาน (Report) ไปยังแพลตฟอร์มตามช่องทางที่จัดไว้ให้

10. ก่อนที่เพิ่มเพื่อน หรือพูดคุยผ่านช่องทางสื่อสังคมออนไลน์ ต้องมั่นใจว่าบัญชีของผู้นั้นเป็นของบุคคลที่รู้จักจริง ๆ ไม่ใช่เป็นบุคคลอื่นที่ปลอมตัวมา หากมีการพูดคุย (Chat) และเกิดความสงสัย เช่น การขอยืมเงิน ควรที่จะติดต่อบุคคลนั้นผ่านช่องทางอื่นเพื่อทำการยืนยัน เช่น การพูดคุยทางโทรศัพท์ หรือทางวีดีโอคอล เพื่อยืนยันเสียง และหน้าตา เป็นต้น

11. ตั้งค่าการยืนยันตัวตนแบบสองปัจจัย (Two-Factor Authentication) เพื่อป้องกันการถูกขโมยบัญชี

12. เคารพความเป็นส่วนตัวของผู้อื่นเสมอ โดยเฉพาะกับเด็ก และเยาวชน

13. ติดตามข่าวสารในเรื่องอาชญากรรมทางไซเบอร์ (Cybercrime) อย่างสม่ำเสมอเพื่อที่จะไม่ได้ตกเป็นเหยื่อ

14. ใช้สัญชาตญาณ และสามัญสำนึกเป็นหลักในการตัดสินเมื่อพบสิ่งที่สงสัย ถ้าไม่แน่ใจ ควรขอคำปรึกษาจากผู้ที่ไว้ใจได้

10.5. การระรานทางไซเบอร์ (Cyberbullying)

Cyberbullying เกิดขึ้นได้ทุกที่ ทุกเวลา และสามารถทำร้ายเหยื่อทั้งทางร่ายการ และจิตใจได้ Cyberbullying อยู่ในรูปแบบของทั้งตัวอักษร รูปภาพ หรือสื่อในรูปแบบใด ๆ การกระทำ Cyberbullying ที่แม้ว่าไม่ได้ระบุข้อมูลส่วนบุคคลของเหยื่อโดยตรง เช่น ไม่ระบุชื่อตรง ๆ ก็ยังถือว่าเป็นการ Cyberbullying และผู้กระทำไม่สามารถปฏิเสธการกระทำนั้นได้

ขั้นตอนปฏิบัติ

10.5.1. การสื่อสาร และให้ความรู้

1. เมื่อพบการ Cyberbullying ควรรายงานเหตุทันที ไม่ว่าผู้ที่พบเห็นจะเป็นเหยื่อโดยตรง หรือไม่ก็ตาม

2. การ Cyberbullying นั้นแม้ว่าผู้กระทำจะไม่ได้ตั้งใจ ก็ยังถือว่าเป็น Cyberbullying ดังนั้น จึงต้องระมัดระวังในการโพสต์ หรือส่งข้อความใด ๆ ที่มีการกล่าวถึงบุคคลอื่น

10.5.2. สัญญาณการเกิด Cyberbullying

1. หยุดการใช้งานสื่อสังคมออนไลน์อย่างคาดไม่ถึง หรือหยุดการเข้าในกิจกรรมออนไลน์ เช่น การออกจากกลุ่มแชททันที

2. มีการทะเลาะเบาะแว้ง มีอารมณ์ฉุนเฉียว โกรธ กดดัน หรือแปรปรวน ในโลกออนไลน์

3. ปรากฏตัวในที่ทำงานน้อยลง

4. มีการยกเลิกการเป็นเพื่อนในสังคมออนไลน์ หรือตีตัวออกห่างจากเพื่อนที่ทำงานในชีวิตจริง

10.5.3. ข้อแนะนำเมื่อถูก Cyberbullying

1. เซฟ (Save) ข้อความ หรือสื่อใด ๆ ที่เป็นการ Cyberbullying และไม่ลบทิ้ง

2. ไม่ตอบกลับ

3. รายงานไปยังผู้ที่เกี่ยวข้องเพื่อดำเนินการตามขั้นตอนต่อไป

4. ปรึกษาในช่องทางที่จัดขึ้นเพื่อให้ความช่วยเหลือต่าง ๆ เช่น คำปรึกษา หรือเยียวยาทางจิตใจ เป็นต้น

ตารางที่ 17 แบบประเมินตนเองการถูกระรานทางไซเบอร์ (Cyberbullying)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้น ซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. คำจำกัดความ และขอบเขต		
• หน่วยงานเคยมีการสื่อสารเรื่อง Cyberbullying หรือไม่		
• หน่วยงานได้กำหนดขอบเขตของ Cyberbullying หรือไม่ ว่ามีรูปแบบ และวิธีใดบ้าง		
2. การสร้างความตระหนัก		
• หน่วยงานได้มีการฝึกอบรมในเรื่องที่เกี่ยวกับ Cyberbullying หรือไม่		
• หน่วยงานได้มีการวัดผลว่าการฝึกอบรมดังกล่าว ได้ช่วยลดการ Cyberbullying ลง หรือไม่		
3. การรายงาน		
• หน่วยงานได้มีการสื่อสารว่าเมื่อใดถึงจะต้องรายงานไปยังผู้ที่เกี่ยวข้องเมื่อเกิดการ Cyberbullying ไม่ว่าจะเป็นเหยื่อ หรือพบเห็น หรือไม่		
• หน่วยงานได้มีระบบสำหรับรายงาน Cyberbullying ที่มีความปลอดภัยสูง สามารถปกป้องข้อมูลส่วนบุคคลของผู้ที่เกี่ยวข้องได้ หรือไม่		
4. การสืบสวน และตอบสนอง		
• หน่วยงานมีกระบวนการสืบสวน และสอบสวนการ Cyberbullying หรือไม่		
• หน่วยงานมีกระบวนข้างต้นที่ทำได้อย่างรวดเร็ว สามารถเยียวยาเหยื่อ และมีการดำเนินการแก่ผู้กระทำ (เช่น การลงโทษ) อย่างเหมาะสม หรือไม่		
5. การปกป้องข้อมูลส่วนบุคคล		
• หน่วยงานมีกระบวนการปกป้องข้อมูลส่วนบุคคลของผู้ที่เกี่ยวข้องตั้งแต่ต้นจนจบกระบวนการ (หรือตลอดไป) หรือไม่		
6. การบังคับใช้นโยบาย		
• หน่วยงานมีนโยบาย หรือระเบียบที่เกี่ยวกับ Cyberbullying หรือไม่		
• หน่วยงานเคยได้บังคับใช้นโยบายในการจัดการกับ Cyberbullying รวมถึงการดำเนินการกับผู้กระทำ หรือไม่		
7. การให้การสนับสนุน		

คำถาม	ใช่	ไม่ใช่
• หน่วยงานได้มีการจัดให้คำปรึกษาเพื่อช่วยเหลือเหยื่อ Cyberbullying ไม่ว่าจะเป็นการเยียวยาจิตใจ หรือการจัดหานักจิตวิทยาเพื่อให้คำปรึกษา หรือไม่		
• หน่วยงานได้มีการจัดให้คำปรึกษาข้างต้นที่ผู้ที่ต้องการรับคำปรึกษา (เช่น เหยื่อ) สามารถเข้าถึงได้ง่าย หรือไม่		
8. การตรวจสอบ และประเมิน		
• หน่วยงานได้มีระบบในการตรวจสอบเหตุ Cyberbullying อย่างสม่ำเสมอ หรือไม่		
9. การมีส่วนร่วม		
• หน่วยงานได้สนับสนุนการมีส่วนร่วม เช่น การสร้างกลุ่มอาสาสมัคร (Community) เพื่อสร้างกิจกรรมการให้ความรู้ และการสร้างพฤติกรรมที่ดีในโลกออนไลน์เพื่อป้องกันปัญหา Cyberbullying หรือไม่		

10.6. แนวทางการตั้งรหัสผ่าน (Password Tips)

รหัสผ่าน (Password) มักถูกใช้ในการยืนยันตัวตนก่อนเข้าสู่ระบบสารสนเทศใด ๆ ดังนั้นการตั้ง Password จะต้องตั้งบนพื้นฐานที่ว่าเจ้าตัวจะรู้อยู่คนเดียว คนอื่นไม่สามารถคาดเดาได้ ซึ่งมีแนวปฏิบัติดังนี้

ข้อควรปฏิบัติ

1. Password ยิ่งยาว ยิ่งดี
2. Password ควรมีจำนวนอักขระขั้นต่ำ 8 ตัว ไม่มีคำซ้ำ และ ไม่มีตัวอักษร หรือตัวเลขที่เรียงกัน
3. Password ไม่ควรจะมีคำที่มีความหมาย หรือพบใน Dictionary และไม่ใช่ชื่อเฉพาะที่เป็นที่รู้จัก
4. ไม่จด Password ลงในกระดาษ หรือในที่ที่ผู้อื่นสามารถเห็นได้ง่าย
5. ควรพิจารณาใช้การยืนยันตัวตนปัจจัยอื่นร่วมด้วย (Two-Factor Authentication) เช่น OTP เพื่อเพิ่มความยาก และซับซ้อนที่ผู้อื่นจะเข้าถึงได้ วิธีนี้เหมาะสำหรับระบบสารสนเทศที่มีความสำคัญสูง เช่น ระบบธนาคาร
6. พิจารณาใช้โปรแกรมบริหารจัดการ Password (Password Management หรือ Password Vault) ซึ่งเป็นโปรแกรมจัดเก็บรหัสผ่าน และมีการเข้ารหัสแบบปลอดภัย ซึ่งจะช่วยให้ผู้ใช้งานไม่ต้องจำ Password ที่หลากหลายของตนเอง ผู้ใช้งานเพียงแค่จำ Password หลัก (Master Password) เท่านั้น แต่ทั้งนี้ก็มีข้อเสียคือ หากมีผู้อื่นสามารถขโมย Master Password ไปได้ ผู้นั้นก็จะสามารถเข้าถึงบัญชีในระบบอื่น ๆ ได้ไปด้วย ดังนั้นผู้ที่ใช้โปรแกรมนี้จะต้องมีความรู้ในการใช้งาน และมีความระมัดระวังเป็นอย่างมาก
7. นอกจากนี้ ผู้ใช้งานควรที่จะตั้ง Password ในการใช้งานอุปกรณ์พกพา เช่น โน้ตบุ้ค โทรศัพท์มือถือ หรือแท็ปเล็ต ด้วย ไม่ว่าจะให้กรอก Password เมื่อเปิดเครื่อง หรือเมื่อ Unlock หน้าจอ เป็นต้น

10.7. การหลอกลวง (Scam)

การหลอกลวง (Scam) เพื่อที่จะขโมยเงิน หรือทรัพย์สินของเหยื่อนั้น ได้เกิดขึ้นมาอย่างยาวนาน และการหลอกลวงสามารถอยู่ในรูปแบบต่าง ๆ ไม่ว่าจะผ่านทางไซเบอร์ หรือช่องทางอื่น ๆ เช่น ทางโทรศัพท์ (เช่น แก๊งคอลเซ็นเตอร์) มิจฉาชีพ (Scammer) มักจะใช้วิธีหว่านล้อม ข่มขู่ หลอกให้รัก หรือหลอกลวงด้วยวิธีใด ๆ ที่ทำให้เหยื่อเชื่อจนทำให้เหยื่อทำตามที่โจรบอก และท้ายสุด เหยื่อก็จะสูญเสียเงินหรือทรัพย์สินไป ในหัวข้อนี้จะนำเสนอตัวอย่างของการหลอกลวง และวิธีการตอบสนอง

ตัวอย่าง: หลอกรักออนไลน์ (หลอก รัก ลวง หลบหนี)

โจรติดต่อผ่านช่องทางออนไลน์ เช่น แชท อีเมล หรือโซเชียลมีเดีย หลอกลวงด้วยการหว่านล้อมเหยื่อเพื่อตีสนิท และหลอกลวงให้เหยื่อหลวงเชื่อว่าจะแต่งงานและใช้ชีวิตร่วมกัน เมื่อเหยื่อหลงเชื่อ โจรจะหลอกลวงเพื่อเอาทรัพย์สินหรือผลประโยชน์จากเหยื่อ และเมื่อเหยื่อเริ่มรู้ตัว โจรก็จะหลบหนี ไม่สามารถติดต่อได้ ปิดช่องทางติดต่อทุกช่องทาง

วิธีวิเคราะห์: เป็นลักษณะการหลอกให้รักผ่านช่องทางออนไลน์ หรือเรียกว่า Romance Scam เนื่องจากเป็นการแสดงความรักอย่างรวดเร็วเกินจริง โดยที่ไม่เคยพบกันมาก่อน และที่สำคัญ ทางฝั่งโจรมีการขอความช่วยเหลือเรื่องเงิน

วิธีตอบสนอง: หากมั่นใจว่าเป็นการหลอกลวง ควรหยุดการติดต่อทันที และปรึกษาคนใกล้ชิด หากไม่มั่นใจต้องหาโอกาสที่จะพบตัวจริงหรือวีดีโอคอล และต้องไม่ให้ทรัพย์สินเด็ดขาด ทั้งนี้ต้องระวังเรื่องความปลอดภัยในชีวิตด้วย

ตัวอย่าง: พัสดุค้าง (ความกังวล)

มีสายโทรศัพท์เข้ามา ปลายสายแจ้งว่าเป็นบริษัทส่งพัสดุถึงเรา แต่พัสดุยังคงค้างอยู่ที่ ตม. ให้เราโอนเงิน 3,000 บาท ถึงจะนำพัสดุออกมาได้

วิธีวิเคราะห์: บริษัทพัสดุไม่มีนโยบายเก็บเงินลักษณะนี้

วิธีตอบสนอง: วางสาย ไม่โต้ตอบ และต้องไม่กระทำการใด ๆ ไม่ว่าจะแอด LINE ดาวน์โหลดแอปฯ กด Link สแกน QR Code หรือโอนเงินใด ๆ

ตัวอย่าง: พัวพันกับคดี (ความกลัว)

มีสายโทรศัพท์เข้ามา ปลายสายแจ้งว่าเป็นตำรวจ และหาว่าเราพัวพันกับคดี และมีการโอนสายให้คุยกับตำรวจคนอื่น ๆ อีกเพื่อยืนยันว่าเป็นเรื่องจริง และให้เราแอด LINE และคลิก Link เพื่อกรอกข้อมูลเพิ่มเติม

วิธีวิเคราะห์: ตำรวจไม่จับคนร้ายด้วยวิธีนี้

วิธีตอบสนอง: วางสาย ไม่โต้ตอบ และต้องไม่กระทำการใด ๆ ไม่ว่าจะแอด LINE ดาวน์โหลดแอปฯ กด Link สแกน QR Code หรือโอนเงินใด ๆ

ตัวอย่าง: ถูกรางวัล (ความโลภ)

มี LINE จากบุคคลที่ไม่รู้จัก แจ้งว่าเราถูกรางวัลจากการจับรางวัลเครื่องดื่มยี่ห้อหนึ่ง และเราจะต้องเสียภาษีก่อน 5,000 บาท ถึงจะได้รางวัล และจะต้องโอนค่าภาษีภายใน 10 นาที ไม่เช่นนั้นถือว่าสละสิทธิ์

วิธีวิเคราะห์: บริษัท หรือภาคธุรกิจไม่ใช้วิธีที่เร่งรีบแบบนี้

วิธีตอบสนอง: ไม่โอนเงิน หรือกระทำการใด ๆ ที่ปลายสายบอก ถ้าเราเคยเข้าร่วมชิงรางวัลนั้นจริง ควรตรวจสอบกับบริษัท หรือภาคธุรกิจนั้นด้วยตนเองเพื่อยืนยัน

ตัวอย่าง: แจ้งว่ามาจากหน่วยงานภาครัฐ และชวนคุยโดยที่ยังไม่รู้วัตถุประสงค์ (ความกังวล)

มีสายโทรศัพท์เข้ามา ปลายสายแจ้งว่ามาจากกรมที่ดิน และทราบข้อมูลของเราทุกอย่างตั้งแต่ชื่อ นามสกุล หมายเลขบัตรประชาชน ที่อยู่ และข้อมูลส่วนบุคคลอื่น ๆ ที่เกี่ยวข้องกับที่อยู่อาศัยของเรา ปลายสายมีการพูดคุยเรื่องระเบียบทั่วไป รวมถึงการเสียภาษีที่ดิน ปลายสายไม่เร่งรีบที่จะให้เสียภาษี และให้เพิ่มเพื่อนใน LINE เพื่อติดต่ออีกครั้งในวันพรุ่งนี้ จากนั้น วันรุ่งขึ้น ก็โทรมาอีกครั้ง

วิธีวิเคราะห์: กรมที่ดินไม่มีแนวปฏิบัติแบบนี้ และเรามั่นใจว่าเราเสียภาษีที่ดิน หรือที่อยู่อาศัยตามช่องทางที่ถูกต้องทุกปีอยู่แล้ว กรณีนี้ปลายสายจะไม่เร่งรีบเพื่อล่อให้เหยื่อหลงเชื่อ และตายใจ

วิธีตอบสนอง: วางสาย ไม่แอด LINE หรือกระทำการใด ๆ ที่ปลายสายบอก หากไม่มั่นใจ ให้โทรติดต่อกับหน่วยงานที่ถูกกล่าวอ้างเพื่อยืนยัน แต่จำไว้เสมอว่า ในการติดต่อกลับ ต้องติดต่อกลับด้วยช่องทางที่ถูกต้องเท่านั้น (เช่น เบอร์โทรหน่วยงานนั้นที่ปรากฏในเว็บไซต์ของหน่วยงาน) ไม่ใช่ติดต่อกลับไปยังเบอร์โทรศัพท์ หรือ LINE ที่ปลายสายได้ให้เอาไว้

ตัวอย่าง: ถูกเรียกค่าไถ่ข้อมูล หรือ Ransomware (ความกลัว และกังวล)

ได้รับอีเมลจากบุคคลที่ไม่รู้จัก ข่มขู่ว่าได้ข้อมูลลับจากบริษัทของเรา และจะเผยแพร่ข้อมูลสู่สาธารณะ ให้เราจ่ายเงินค่าไถ่ 300,000 บาทเป็นค่าไถ่ข้อมูล

วิธีวิเคราะห์: อาจจะจริง หรือไม่จริงก็ได้

วิธีตอบสนอง: ไม่จ่ายเงิน เพราะไม่มีการรับประกันใด ๆ ว่าถ้าจ่ายแล้ว โจรจะทำตามที่บอก แจ้งตำรวจ ตรวจสอบว่าสิ่งที่โจรบอกเป็นจริง หรือไม่ ตรวจสอบระบบความมั่นคงปลอดภัยของบริษัทอีกครั้งเพื่อป้องกันไม่ให้เกิดเหตุการณ์ในอนาคต

สัญญาณที่บ่งบอกว่าอาจจะเกิดการหลอกลวง

1. การแจ้งว่าได้รับรางวัล เช่น มีการแจ้งว่าเราได้รางวัลอย่างง่ายดาย โดยที่เราไม่เคยเข้าร่วมการชิงรางวัลนั้น
2. การร้องขอแบบเร่งด่วน (ปัจจุบันอาจจะไม่เร่งแล้ว เพื่อให้เหยื่อตายใจ) เช่น มีการอ้างว่าเป็นเพื่อน และขอยืมเงินด่วนทันที เพื่อไม่ให้เรามีเวลาตั้งสติ หรือมีเวลาไปตรวจสอบข้อมูล
3. การกำหนดกรอบเวลา หรือมีระยะเวลาที่จำกัด เช่น มีการแจ้งว่าต้องโอนค่าภาษีเงินรางวัลภายใน 5 นาที มิฉะนั้นจะถือว่าสละสิทธิ์รางวัล
4. การเล่นกับความรู้สึก เช่น การหลอกว่าเป็นผู้เจ็บป่วยเพื่อให้เราสงสาร และบริจาคเงิน
5. การข่มขู่ เช่น การปลอมเป็นตำรวจเพื่อข่มขู่ให้เราดำเนินการใด ๆ อันจะนำพาไปสู่การเสียทรัพย์

ทั้งนี้หากท่านตกเป็นเหยื่อแล้ว จะต้องแจ้งเหตุตามช่องทางต่อไปนี้

- แจ้งความออนไลน์ คดีอาชญากรรมทางเทคโนโลยี https://thaipoliceonline.go.th/ หรือ ศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ (Anti Online Scam Operation Center: AOC) สายด่วน 1441
- แจ้งเหตุการณ์การตกเป็นเหยื่อการทำธุรกรรมออนไลน์ ได้ที่ศูนย์รับเรื่องร้องเรียนปัญหาออนไลน์ (1212 Online Complaint Center หรือ 1212 OCC) ภายใต้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) https://1212etda.com/

11. ข้อแนะนำด้านความมั่นคงปลอดภัยสำหรับการเปลี่ยนแปลงเป็นดิจิทัล (Security for Digital Transformation)

การเปลี่ยนแปลงเป็นดิจิทัล (Digital Transformation) ช่วยให้ชีวิตเราสะดวก รวดเร็ว และมีประสิทธิภาพมากขึ้น แต่ในขณะเดียวกันก็มาพร้อมกับความเสี่ยงด้านความปลอดภัยทางไซเบอร์ ข้อมูลส่วนตัวของเรา เอกสารสำคัญของหน่วยงาน ธุรกรรมทางการเงิน ล้วนถูกจัดเก็บ และใช้งานในรูปแบบดิจิทัล ดังนั้น การสร้างเกราะป้องกันที่แข็งแกร่งจึงเป็นสิ่งจำเป็น

การรักษาความปลอดภัยในยุคดิจิทัลนั้น ไม่ใช่เพียงแค่การมีระบบรักษาความปลอดภัยพื้นฐาน แต่ต้องมองภาพรวมตั้งแต่ความเข้าใจอย่างลึกซึ้งในบริบทของหน่วยงาน การออกแบบระบบให้ปลอดภัยตั้งแต่ต้น ใช้เทคโนโลยีเข้ารหัสข้อมูล สร้างวัฒนธรรมความปลอดภัยภายในหน่วยงาน ไปจนถึงการมีแผนรับมือ

และแก้ไขกรณีเกิดเหตุโจมตีทางไซเบอร์ ความปลอดภัยในโลกดิจิทัลต้องอาศัยความร่วมมือจากทุกภาคส่วน ทั้งภาครัฐ ภาคเอกชน และประชาชนผู้ใช้งาน ร่วมกันสร้างสังคมดิจิทัลที่ปลอดภัย ไร้กังวล

ขั้นตอนปฏิบัติ

1. **กำหนดวัตถุประสงค์ทางธุรกิจ (Business Objective) ชัดเจน** ก่อนนำเทคโนโลยีใด ๆ เข้ามาใช้ ให้นิยามเป้าหมายทางธุรกิจที่ต้องการ เช่น เพิ่มยอดขาย ปรับปรุงประสิทธิภาพ ลดต้นทุน จากนั้นประเมินความสำคัญของ Confidentiality (การรักษาความลับของข้อมูล), Integrity (การรักษาความสมบูรณ์ของข้อมูล) และ Availability (การรักษาสภาพพร้อมใช้งานของข้อมูล) ในบริบทนั้น ๆ ตัวอย่างเช่น ธุรกิจการเงินที่เน้นข้อมูลบัตรเครดิต อาจให้ความสำคัญกับ Confidentiality สูงสุด ในขณะที่ธุรกิจบริการออนไลน์ที่เน้น Uptime อาจให้ความสำคัญกับ Availability มากกว่า
2. **ออกแบบระบบให้ปลอดภัยตั้งแต่ต้น (Security by Design)** แทนที่จะเพิ่มระบบรักษาความปลอดภัยทีหลัง ให้บูรณาการแนวคิดนี้เข้าไปทุกขั้นตอน ตั้งแต่การวิเคราะห์ความเสี่ยง การเลือกเทคโนโลยี และการเขียนโค้ด ตัวอย่างเช่น ใช้การเข้ารหัสข้อมูลตั้งแต่ตอนสร้าง จัดการสิทธิ์การเข้าถึงอย่างละเอียด และออกแบบระบบให้ทนทานต่อการโจมตี ผู้สนใจสามารถอ่านรายละเอียดทางเทคนิคในบทที่ 9 ประกอบ
3. **ควบคุมการเข้าถึงข้อมูลอย่างเข้มงวด** ใช้หลักการการให้สิทธิให้น้อยที่สุดเท่าที่จำเป็น (Least Privilege) คือ มอบสิทธิ์การเข้าถึงขั้นต่ำสุดที่จำเป็นสำหรับแต่ละบุคคล ไม่ใช่ให้สิทธิ์แบบ All-Access Control ตัวอย่างเช่น พนักงานฝ่ายบัญชีสามารถเข้าถึงข้อมูลการเงินได้ แต่ไม่สามารถแก้ไขข้อมูลลูกค้า
4. **ใช้เทคโนโลยีเข้ารหัสข้อมูล** ปกป้องข้อมูลสำคัญทั้งขณะส่งผ่าน (Data in Transit) ด้วยโปรโตคอลที่ปลอดภัยอย่าง TLS/SSL และขณะจัดเก็บ (Data at Rest) ด้วยวิธีการเข้ารหัสแบบ AES หรือ RSA
5. **อัพเดตระบบ และซอฟต์แวร์ให้ทันสมัย** ติดตั้ง Patch ความปลอดภัยทันทีที่มีอัพเดต ปิดการใช้งานซอฟต์แวร์เก่าที่ไม่ได้รับการสนับสนุนอีกต่อไป สร้างกระบวนการอัพเดตอัตโนมัติเพื่อความรวดเร็ว
6. **สำรองข้อมูลเป็นประจำ** วางแผนสำรองข้อมูล (Backup) ด้วยหลักการ 3-2-1 คือ
    - สำรองข้อมูล 3 ชุด (3 Copies)

- เก็บสำรองข้อมูลไว้ใน 2 รูปแบบ (2 Formats) เช่น ฮาร์ดดิสก์ และคลาวด์
- เก็บสำรองข้อมูลไว้ใน 1 สถานที่ที่อยู่คนละที่ (1 Offsite Location) เพื่อป้องกันภัยพิบัติ

และจะต้องทดสอบการกู้คืนข้อมูลเพื่อให้แน่ใจว่าสามารถกู้คืนข้อมูลได้สำเร็จได้ทันท่วงที กรณีเกิดเหตุการณ์ไม่คาดคิดอีกด้วย

7. สร้างวัฒนธรรมความปลอดภัยภายในหน่วยงาน ส่งเสริมให้พนักงานตระหนักถึงความสำคัญของความปลอดภัย จัดกิจกรรมสร้างความรู้ อบรมพนักงานให้รู้จักวิธีการรับมือกับภัยไซเบอร์ และรายงานเหตุการณ์ที่น่าสงสัย

8. จัดฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ให้พนักงาน การอบรมนี้ไม่ควรออกแบบเป็นหลักสูตรเดียวสำหรับพนักงานทุกคน แต่ควรออกแบบให้ตรงกับสายงาน และความรับผิดชอบของแต่ละคน เช่น พนักงานฝ่ายไอทีต้องรู้จักวิธีการรักษาความปลอดภัยระบบซึ่งลงลึกทางเทคนิค ขณะที่พนักงานฝ่ายขายต้องรู้จักความตระหนักในภาพรวม และการตรวจสอบอีเมลฟิชชิ่ง

9. ติดตาม และตรวจสอบระบบอย่างสม่ำเสมอ ตรวจสอบ log ระบบ สัญญาณเตือนภัย และกิจกรรมที่ผิดปกติอย่างต่อเนื่อง ใช้เครื่องมือในการตรวจสอบความปลอดภัย และวิเคราะห์ข้อมูลเพื่อหาแนวโน้มการโจมตี

10. เลือกใช้ผู้ให้บริการที่มีความน่าเชื่อถือ ศึกษา และประเมินมาตรฐานความปลอดภัยของผู้ให้บริการ Cloud หรือบริการอื่น ๆ เลือกผู้ที่มีนโยบายความปลอดภัยชัดเจน มีการรับรองมาตรฐานสากล และมีการกำหนดข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA)

11. กำหนดสิทธิชัดเจนเมื่อต้องจ้างหน่วยงานภายนอก ทำสัญญาระบุสิทธิของผู้ว่าจ้าง (หน่วยงานตนเอง) ในการเข้าถึงข้อมูลของหน่วยงานเอง โดยไม่ต้องเสียค่าใช้จ่ายใด ๆ เพิ่มเติมแก่ผู้รับจ้างหรือผู้ประมวลผลข้อมูล (หน่วยงานภายนอก) นอกจากนี้ยังรวมถึงสิทธิต่าง ๆ ที่รักษาประโยชน์ของหน่วยงานตนเอง เช่น การกำหนดระยะเวลาในการเก็บรักษาข้อมูล (Data Retention) การกำหนดขั้นตอนการโอนย้ายข้อมูล การกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลและการรักษาธรรมภิบาลข้อมูลของผู้ว่าจ้างที่จะต้องสอดคล้องในแนวทางเดียวกันกับหน่วยงานผู้ว่าจ้างหรืออยู่ในระดับที่สูงกว่า เป็นต้น แนวปฏิบัตินี้ยังรวมถึงการดำเนินการด้านข้อมูลร่วมกับหน่วยงานอื่นที่ไม่ใช่เป็นการว่าจ้างอีกด้วย

12. ทำประกันภัยไซเบอร์ ช่วยลดความเสียหายทางการเงินกรณีเกิดเหตุโจมตี ข้อมูลที่สูญหาย ค่าใช้จ่ายในการกู้คืนระบบ และค่าปรับจากกฎหมายคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้หน่วยงานควรวิเคราะห์ความเสี่ยง และความคุ้มค่าในการทำประกันภัย

13. มีแผนรับมือ และแก้ไขกรณีเกิดเหตุ (Incident Response Plan) กำหนดขั้นตอนการดำเนินการกรณีเกิดเหตุโจมตีไว้อย่างชัดเจน มีทีมงานรับผิดชอบชัดเจน รู้วิธีการระบุ เก็บรักษาหลักฐาน และรายงานเหตุการณ์ มีการฝึกซ้อมแผนเป็นประจำเพื่อให้ทีมงานมีความพร้อม รับมือกับสถานการณ์จริงได้อย่างรวดเร็ว และทดสอบแผนเป็นระยะเพื่อประเมินประสิทธิภาพ และปรับปรุงให้เหมาะสม

14. ติดตามแนวโน้มภัยคุกคามใหม่ ๆ ติดตามข่าวสารด้านความปลอดภัยไซเบอร์จากแหล่งที่เชื่อถือได้ทั้งจากหน่วยงานภาครัฐ หรือเอกชน ทำการประเมินความเสี่ยงจากภัยคุกคามใหม่ ๆ และปรับแผนป้องกันให้ทันสมัย และใช้เครื่องมือ หรือเทคโนโลยีในการรับมือภัยคุกคามที่เหมาะสมกับบริบทหน่วยงาน

15. ร่วมมือกับหน่วยงานที่เกี่ยวข้อง และผู้มีส่วนได้เสีย แลกเปลี่ยนข้อมูลภัยคุกคามกับหน่วยงานที่เกี่ยวข้อง เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อช่วยเหลือกัน และกันในการร่วมป้องกัน และรับมือกับภัยไซเบอร์ เพื่อให้มีการติดตามสืบสวน และป้องกันการโจมตีในวงกว้าง รวมถึงรายงานเหตุการณ์โจมตีไซเบอร์ให้กับหน่วยงานที่รับผิดชอบ ตามที่กฎหมายกำหนด และต้องสื่อสารกับผู้มีส่วนได้เสีย หรือผู้ที่มีโอกาสได้รับผลกระทบต่อภัยคุกคาม นอกจากนี้ควรหาโอกาสเข้าร่วมกิจกรรมอบรม และสัมมนาเพื่อแลกเปลี่ยนความรู้ และประสบการณ์ด้านความปลอดภัยกับหน่วยงานอื่น ๆ เพื่อสร้างความร่วมมือ

16. ทดสอบระบบรักษาความปลอดภัยเป็นประจำ ประเมินประสิทธิภาพของระบบรักษาความปลอดภัยเพื่อหาช่องโหว่ที่อาจถูกโจมตี ปรับปรุง และอุดช่องโหว่ที่พบเจอให้รวดเร็ว และทดสอบแผนรับมือและแก้ไขกรณีเกิดเหตุเป็นประจำเพื่อให้ทีมงานมีความพร้อม ในส่วนของการทดสอบนี้ควรกระทำโดยผู้เชี่ยวชาญไม่ว่าจะจากภายใน หรือภายนอก และผู้ทดสอบต้องไม่มีบทบาทที่ขัดกัน (Role Conflict) เช่น ผู้ทดสอบระบบจะต้องไม่มีบทบาทใด ๆ ในการพัฒนาระบบเดียวกัน

ตารางที่ 18 แบบประเมินตนเองด้านความมั่นคงปลอดภัยสำหรับการเปลี่ยนแปลงเป็นดิจิทัล (Security for Digital Transformation)

** แบบประเมินตนเองนี้ เป็นเพียงการประเมินความพร้อมในระดับขั้นพื้นฐานเท่านั้น ซึ่งหน่วยงานที่มีความพร้อม ควรจะมีการประเมินเป็น "ใช่" ครบทุกข้อ และหากข้อใดมีคำตอบเป็น "ไม่ใช่" หน่วยงานควรจะมีการดำเนินการในข้อนั้นอย่างเหมาะสม แม้ว่าหน่วยงานจะมีการประเมินเป็น "ใช่" ทุกข้อ ก็ยังไม่ได้หมายความว่าหน่วยงานนั้นสามารถวางใจได้และไม่ดำเนินการใด ๆ ต่อ แต่หน่วยงานยังคงต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยต่อไป และมีการปรับปรุงการดำเนินการอยู่เสมอ*

คำถาม	ใช่	ไม่ใช่
1. หน่วยงานมีประเมินความสำคัญของ Confidentiality (ข้อมูลลับ), Integrity (ความถูกต้อง) และ Availability (การเข้าถึงได้) ตามวัตถุประสงค์ทางธุรกิจ (Business Objective) หรือไม่		
2. หน่วยงานยึดหลักการออกแบบระบบให้ปลอดภัยตั้งแต่ต้น (Security by Design) ในการพัฒนาระบบความมั่นคงปลอดภัย หรือไม่		
3. หน่วยงานมีการควบคุมการเข้าถึงข้อมูลอย่างเข้มงวดในรูปแบบ Least Privilege หรือไม่		
4. หน่วยงานมีการพิจารณาการเข้ารหัสข้อมูลที่เหมาะสมทั้งขณะส่งผ่าน (Data in Transit) และขณะจัดเก็บ (Data at Rest) หรือไม่		
5. หน่วยงานมีการอัพเดตระบบ และซอฟต์แวร์ให้ทันสมัย หรือไม่		
6. หน่วยงานมีการสำรองข้อมูล (Backup) เป็นประจำแบบ 3-2-1 หรือไม่		
7. หน่วยงานมีการจัดฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์แก่พนักงานเป็นประจำ หรือไม่		
8. หน่วยงานมีการติดตาม และตรวจสอบความปลอดภัยของระบบอย่างสม่ำเสมอ หรือไม่		
9. หน่วยงานมีกระบวนการคัดเลือกผู้ให้บริการที่มีความน่าเชื่อถือ และมีการกำหนด SLA หรือไม่		
10. หน่วยงานมีแผนรับมือ และแก้ไขกรณีเกิดเหตุ (Incident Response Plan) หรือไม่		
11. หน่วยงานมีการสร้างความร่วมมือ และติดต่อสื่อสารกับหน่วยงานที่เกี่ยวข้อง และผู้มีส่วนได้เสีย เป็นประจำ หรือไม่		
12. หน่วยงานมีการทดสอบระบบรักษาความปลอดภัยเป็นประจำ หรือไม่		

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
www.dga.or.th