ประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม

ฉบับวันที่ 7 ธันวาคม 2565

จัดทำโดย
สำนักกำกับดูแลกิจการโทรคมนาคม (ดท.)
สำนักงาน กสทช.

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

บทนำ

ด้วยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้หน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จัดทำประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม (สำนักงาน กสทช.) ในฐานะหน่วยงานกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านเทคโนโลยีสารสนเทศและโทรคมนาคม จึงต้องจัดทำประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านเทคโนโลยีสารสนเทศและโทรคมนาคมถือปฏิบัตินอกเหนือจากต้องปฏิบัติตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ 2564 ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

อย่างไรก็ดี แนวทางการจัดทำประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ดังกล่าวมาจากข้อเสนอในรายงาน “โครงการจ้างที่ปรึกษาดำเนินการศึกษาและตรวจสอบขั้นตอนการปฏิบัติการรักษาความปลอดภัยไซเบอร์และข้อมูลส่วนบุคคลของผู้ประกอบกิจการโทรคมนาคม” (มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ) ของสำนักงาน กสทช. ซึ่งได้ดำเนินการศึกษา วิเคราะห์แนวทางการบริหารจัดการที่ดี กรอบการดำเนินงาน หลักปฏิบัติตามมาตรฐานสากล และจัดทำประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นประมวลแนวปฏิบัติฯ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านเทคโนโลยีสารสนเทศและโทรคมนาคม โดยอ้างอิงจากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ ๒๕๖๔ จาก สกมช. และสำนักงาน กสทช. ได้จัดให้มีการร่วมแสดงความคิดเห็นประมวลแนวปฏิบัติฯ ดังกล่าว จำนวน ๒ ครั้ง ได้แก่ วันที่ ๓๐ พฤษภาคม ๒๕๖๕ และวันที่ ๒๘ มิถุนายน ๒๕๖๕ จากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านเทคโนโลยีสารสนเทศและโทรคมนาคมทุกรายและหน่วยงานที่เกี่ยวข้อง ทั้งนี้ เพื่อให้สามารถปฏิบัติไปในทิศทางเดียวกัน และสอดคล้องตามมาตรฐานสากล

วัตถุประสงค์

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านเทคโนโลยีสารสนเทศและโทรคมนาคมปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

สอดคล้องกับมาตรฐานสากล และสนับสนุนการดำเนินงานของสำนักงาน กสทช. และ สกมช. เพื่อให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ขอบเขตการใช้

ใช้กับผู้รับใบอนุญาตประกอบกิจการโทรคมนาคมที่สำนักงาน กสทช. ได้กำหนดให้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ตามมาตรา 49 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ถือปฏิบัติ

คำนิยาม

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

	หมายถึง	หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
สำนักงาน กสทช.	หมายถึง	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม
สกมช.	หมายถึง	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
พระราชบัญญัติฯ	หมายถึง	พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
บริการที่สำคัญ	หมายถึง	ภารกิจหรือบริการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ตามมาตรา 49 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

โปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile)

	หมายถึง	การวิเคราะห์เชิงปริมาณ (quantitative analysis) ของประเภทของภัยคุกคามที่องค์กร สินทรัพย์ โครงการ หรือบุคคลเผชิญ เป้าหมายของโปรไฟล์ความเสี่ยงฯ คือ การให้ความเข้าใจความเสี่ยงโดยกำหนดค่าตัวเลขให้กับตัวแปรที่แสดงถึงภัยคุกคามประเภทต่าง ๆ จุดอ่อนที่อาจก่อให้เกิดเหตุการณ์ด้านมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น และอันตรายที่ภัยคุกคามเหล่านั้นจะก่อขึ้น แต่ละองค์กรมีโปรไฟล์ความเสี่ยงเฉพาะของตนเอง โดยพิจารณาจากสินทรัพย์ที่ต้องการปกป้อง เป้าหมายที่ต้องการบรรลุ ความสามารถในการจัดการกับความเสี่ยง และความพร้อมและความสามารถที่จะจัดการกับความเสี่ยง

1. ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประมวลแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีรายละเอียด ดังต่อไปนี้

1.1 แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1.1.1 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ 1 ครั้ง โดยกำหนดให้มีขอบเขตของการตรวจสอบซึ่งรวมถึง :

(ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA)

(ข) บริการที่สำคัญของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นเจ้าของและใช้บริการจากผู้ให้บริการภายนอกตามผลการวิเคราะห์ในข้อ (ก)

(ค) การปฏิบัติตามพระราชบัญญัติฯ และประมวลแนวทางปฏิบัตินี้ และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และทิศทางที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) อาจออกให้

1.1.2 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการดำเนินการ[1] ต่อ สกมช. ภายในสามสิบ (30) วัน นับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในมาตรา 54 แห่งพระราชบัญญัติฯ พร้อมทั้งสำเนาส่งให้สำนักงาน กสทช.

1.1.3 ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา 54 ของพระราชบัญญัติฯ พบว่า มีการไม่ปฏิบัติตามของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกับข้อกำหนดที่ระบุไว้ในพระราชบัญญัติฯ หรือประมวลแนวทางปฏิบัติ หรือมาตรฐานการปฏิบัติงานที่ออกภายใต้พระราชบัญญัติฯ เว้นแต่ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) จะระบุเป็นลายลักษณ์อักษรเป็นอย่างอื่น ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศส่งแผนการดำเนินการแก้ไขไปยัง สกมช. ภายในสามสิบ (30) วันทำการนับถัดจากวันที่ได้รับรายงานการตรวจสอบ โดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้

(ก) ให้รายละเอียดการดำเนินการแก้ไขที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตามทั้งหมด

(ข) กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อย่อย (ก)

1.1.4 ในกรณีที่ กกม. เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยัง สกมช. ภายในระยะเวลาที่ กกม. กำหนด พร้อมทั้งสำเนาส่งให้สำนักงาน กสทช. ด้วย

1.1.5 เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กกม. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะต้องดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้เสร็จสิ้นภายในระยะเวลาตามที่ระบุไว้ในนั้นเพื่อผ่านเกณฑ์พิจารณาของ กกม.

---

[1]รูปแบบสรุปรายงานการตรวจสอบ สกมช. จะกำหนดรายละเอียดในการดำเนินการต่อไป เพื่อให้การรายงานตรวจสอบสามารถเปรียบเทียบกันได้ การประเมินผลและประเมินความเสี่ยงในภาพรวมสามารถทำได้มีประสิทธิภาพมากขึ้น

1.2 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและต่อเนื่อง หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้อง ในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศโดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง และรายงานให้คณะกรรมการหรือผู้มีอำนาจบริหารของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่เกี่ยวข้องได้รับทราบโดยครอบคลุมอย่างน้อย ในเรื่องดังต่อไปนี้

1.2.1 การประเมินความเสี่ยง (Risk Assessment)

(ก) การระบุความเสี่ยง (Risk Identification)

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก โดยระบุอย่างน้อยครอบคลุม

- ผู้กระทำให้เกิดความเสี่ยงและเหตุการณ์ความเสี่ยง เช่น ผู้ไม่ประสงค์ดี ภัยคุกคาม หรือช่องโหว่ เป็นต้น
- ประเภทของความเสี่ยง เช่น ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศความเสี่ยงด้านโปรแกรม ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยงด้านข้อมูล ความเสี่ยงด้านบุคลากร ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ความเสี่ยงด้านการบริหารโครงการ เป็นต้น
- สาเหตุของการเกิดเหตุการณ์ เช่น กระบวนการปฏิบัติงาน ระบบงาน บุคลากร ปัจจัยภายนอก เป็นต้น
- ผลกระทบต่อทรัพย์สิน ทรัพยากร การปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการดำเนินธุรกิจของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ทั้งนี้ ผู้มีส่วนร่วมในการระบุความเสี่ยงด้านเทคโนโลยีสารสนเทศควรมีความรู้และความเข้าใจถึงเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้ระบุไว้เป็นอย่างดี

(ข) การวิเคราะห์ความเสี่ยง (Risk Analysis)

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม โดยเหตุการณ์ความเสี่ยงโดยควรดำเนินการ ดังนี้

- กำหนดเจ้าของความเสี่ยง (Risk Owner)
- ระบุการควบคุมที่มีอยู่ในปัจจุบัน (Existing Control)
- พิจารณาและค้นหาสาเหตุและสถานการณ์ที่เป็นไปได้
- วิเคราะห์ผลกระทบที่เกิดขึ้นจากเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

(ค) การประเมินค่าความเสี่ยง (Risk Evaluation)

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite) โดยควรดำเนินการ ดังนี้

- กำหนดเกณฑ์การประเมินความเสี่ยงด้านโอกาสและผลกระทบ เช่น ด้านการเงิน ด้านปฏิบัติการ เป็นต้น
- กำหนดระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)
- ประเมินค่าโอกาสและผลกระทบของเหตุการณ์ความเสี่ยงที่อาจเกิดขึ้น เพื่อระบุระดับค่าความเสี่ยงของแต่ละเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
- จัดลำดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์แสดงในแผนภาพความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

1.2.2 การจัดการความเสี่ยง (Risk Treatment)

ผู้ประกอบกิจการฯ ต้องกำหนดแนวทางจัดการควบคุมและป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ โดยควรครอบคลุมอย่างน้อย ดังนี้

- กำหนดแนวทางในการจัดการและควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยการเลือกแนวทางในการจัดการและควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ควรพิจารณาถึงความคุ้มค่าและวิธีการที่เหมาะสมสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น การหยุดหรือหลีกเลี่ยงความเสี่ยง การลดหรือบรรเทาโอกาสเกิดความเสี่ยง การลดหรือบรรเทาผลกระทบที่เกิดขึ้น การแบ่งหรือโอนความเสี่ยงให้หน่วยงานอื่น การยอมรับความเสี่ยงไว้โดยแจ้งเหตุผลให้ผู้บริหารทราบเพื่อตัดสินใจในการยอมรับความเสี่ยง เป็นต้น
- ระบุรายละเอียดของงานที่ต้องดำเนินการ ผู้รับผิดชอบ ระยะเวลาที่ใช้ในการดำเนินการ
- ประเมินระดับค่าความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงที่ยอมรับได้
- จัดทำแผนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์โดยจัดลำดับความสำคัญในการดำเนินการ
- นำเสนอและขออนุมัติแผนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
- ดำเนินการสื่อสารแผนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

นอกจากนี้ผู้ประกอบกิจการฯต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator : KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

1.2.3 การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

ผู้ประกอบกิจการฯ ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตามและทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้ โดยควรจัดให้มีการจัดเก็บและบันทึกข้อมูลอย่างเป็นระบบ เพื่อใช้ติดตามและทบทวนความเสี่ยงได้อย่างมีประสิทธิภาพ ครอบคลุมอย่างน้อย

● การติดตามความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

● ประสานงานร่วมกับผู้รับผิดชอบและผู้บริหารถึงสถานะดำเนินงาน อุปสรรคและข้อจำกัดที่เกิดขึ้น

● ศึกษาและวิเคราะห์เหตุการณ์ความเสี่ยงที่เกิดขึ้น รวมทั้งติดตามแนวโน้มของเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและองค์กรอื่น

● รายงานความคืบหน้าของแผนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ตามรอบที่กำหนด

1.2.4 การรายงานความเสี่ยง (Risk Reporting)

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการที่ได้รับมอบหมาย โดยการรายงานควรครอบคลุมอย่างน้อย

● สถานะและผลลัพธ์การดำเนินงานตามแผนการบริหารจัดการ ความเสี่ยงด้านความมั่นคงปลอดภัย ไซเบอร์ประจำปี

● ผลการประเมินและการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์โดยเชื่อมโยงกับความเสี่ยงในระดับองค์กร

● รายงานดัชนีชี้วัดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และรายงานสรุปเหตุการณ์ผิดปกติ

● แนวโน้มความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจจะเกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

● ความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยง

ทั้งนี้ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหาร ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญเช่นกรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ

1.3 แผนการรับมือภัยคุกคามทางไซเบอร์

1.3.1 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องระบุรายละเอียดอย่างน้อย ดังนี้

(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team : CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ โดยอาจเป็นบุคลากรภายในองค์กร หรือบุคคลภายนอกที่มีความเชี่ยวชาญ

(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) โดยหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะต้องกำหนดโครงสร้างการรายงานเมื่อตรวจพบภัยคุกคามทางไซเบอร์ให้กับ สำนักงาน กสทช. และ สกมช.

(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และ CIRT

(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(ช) การติดตามและขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอกหรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืน และการบังคับใช้กฎหมายเพื่อดำเนินคดี

(ฌ) กระบวนการทบทวนหลังการดำเนินการ (After-action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

1.3.2 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

1.3.3 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง ตั้งแต่วันที่แผนได้รับการอนุมัติ

1.3.4 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญหรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

2. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประมวลกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบไปด้วย 5 หัวข้อ ดังนี้

2.1 การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

2.1.1 การจัดการทรัพย์สิน (Asset Management)

2.1.2 การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

2.1.3 การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

2.1.4 การจัดการผู้ให้บริการภายนอก (Third Party Management)

2.2 มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

2.2.1 การควบคุมการเข้าถึง (Access Control)

2.2.2 การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

2.2.3 การเชื่อมต่อระยะไกล (Remote Connection)

2.2.4 สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

2.2.5 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

2.2.6 การแบ่งปันข้อมูล (Information Sharing)

2.3 มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

2.4 มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

2.4.1 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

2.4.2 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

2.4.3 การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

2.5 มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

รายละเอียดแนวปฏิบัติตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มีดังต่อไปนี้

1. การระบุและประเมินความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

1.1 การจัดการทรัพย์สิน (Asset Management)

(1) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญทางสารสนเทศของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

(ก) ชื่อ / คำอธิบายของทรัพย์สิน

(ข) ฟังก์ชันที่สำคัญของทรัพย์สิน

(ค) การระบุและการจัดลำดับความสำคัญ

(ง) เจ้าของและ / หรือผู้ดำเนินการของทรัพย์สิน (Owner)

(จ) ตำแหน่งทางกายภาพของทรัพย์สินแต่ละรายการ

(ฉ) การขึ้นต่อกันของทรัพย์สินบนระบบ / เครือข่ายภายในและ / หรือภายนอก

(ช) ประเภทของอุปกรณ์ ยี่ห้อ

(ซ) หมายเลขอ้างอิงฮาร์ดแวร์ (Serial Number) และหมายเลขอ้างอิงของซอฟต์แวร์ (Software License)

(ฌ) ประเภทการครอบครอง (ซื้อหรือเช่า)

(ญ) วันที่บำรุงรักษาล่าสุด

(ฎ) วันสิ้นสุดการใช้งานตามสัญญา (Warranty) และวันสิ้นสุดการรับประกันการใช้งาน (Support Contract) และ

(ฏ) วันสิ้นสุดการให้บริการจากผู้ผลิต (End of Support)

โดยข้อมูลในรายการ (ช) - (ฏ) ไม่ต้องรายการแก่สำนักงาน กสทช. แต่ต้องมีเก็บไว้เป็นหลักฐานเพื่อให้สามารถตรวจสอบได้

(2) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

(3) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องตรวจสอบ ปรับปรุงทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญใด ๆ

(4) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง

(5) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดกระบวนการหรือแนวปฏิบัติสำหรับการยกเลิกหรือเรียกคืนทรัพย์สิน (Return Asset) เมื่อสิ้นสุดการใช้งาน โดยครอบคลุมทั้งทรัพย์สินที่ใช้งานภายในองค์กร และกรณีที่ผู้ให้บริการภายนอกมีการใช้งานทรัพย์สินขององค์กรทันทีที่มีการยกเลิกสัญญาจ้าง

1.2 การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

(1) ผู้ประกอบกิจการต้องดำเนินการระบุ ประเมิน บริหารจัดการ และติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนด

(2) ทะเบียนความเสี่ยงจะได้รับการปรับปรุงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสารดังต่อไปนี้

(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) ระดับของความเสี่ยง (Level of Risk)

(ฉ) การจัดการความเสี่ยง (Risk Treatment)

(ช) เจ้าของความเสี่ยง (Risk Owner)

(ซ) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)

(ฌ) ความเสี่ยงที่เหลือ (Residual Risk) และ

(ญ) วันที่ทบทวนความเสี่ยง (Date of Risk is Reviewed) (ถ้ามี)

1.3 การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

(1) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดให้มีกระบวนการการบริหารจัดการช่องโหว่ (Vulnerability Management) ของระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) System) ที่เหมาะสมตามระดับความเสี่ยงที่องค์กรประเมิน และให้มีการกำหนดรอบการประเมินช่องโหว่อย่างชัดเจนและสม่ำเสมอ

(2) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดขอบเขตของการประเมินช่องโหว่อย่างน้อย ประกอบด้วย

(ก) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

(ข) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

(ค) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

(3) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องทำการประเมินช่องโหว่ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใดๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใดๆ กับบริการที่สำคัญขององค์กร ทั้งนี้การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

(4) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญขององค์กร โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยงและพิจารณาผลกระทบหรือความเสี่ยงจากการเจาะระบบด้วย

(5) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยเฉพาะอย่างยิ่งทุกระบบที่เป็นมีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

(6) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 ครั้ง ตามความจำเป็น หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ ก่อนที่จะทำการทดสอบระบบใหม่หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยีเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ

(7) ผู้ทดสอบเจาะระบบ (Penetration Tester) ที่ทำหน้าที่เจาะระบบจะต้องได้รับการรับรองและมีประกาศนียบัตร (Accreditations and certifications) ซึ่งเป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ

ในกรณีที่ใช้โปรแกรม (Program) ชุดเครื่องมือ (Tools) หรือบริการ (Service) ในการทดสอบเจาะระบบ ต้องตรวจสอบให้แน่ใจว่าโปรแกรม ชุดเครื่องมือ หรือบริการ เหล่านั้นได้รับการยอมรับ การรับรองและมีการใช้งานอย่างแพร่หลายในกลุ่มอุตสาหกรรม และได้รับมาตรฐานที่เกี่ยวข้อง (ถ้ามี)

(8) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องตรวจสอบให้มั่นใจว่าการระหว่างการทดสอบเจาะระบบทั้งหมดจะต้องดำเนินการภายใต้การดูแลของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(9) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดกระบวนการเพื่อติดตามและจัดการช่องโหว่ที่พบจากการทดสอบเจาะระบบหรือจากการตรวจสอบช่องโหว่ เพื่อให้แน่ใจว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

(10) หากมีการร้องขอรายงานผลการเจาะระบบ จาก กกม. หรือ สกมช. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องส่งรายงานสรุปผลการเจาะระบบ ซึ่งถูกพิจารณาให้เป็นไปตามมาตรา 54 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไปยัง สกมช. พร้อมทั้งสำเนาส่งให้สำนักงาน กสทช. ภายใน 30 วัน นับตั้งแต่วันที่ดำเนินการแล้วเสร็จ โดยจัดทำรายงานสรุปให้อยู่ในรูปแบบรายงานการตรวจสอบที่ สกมช. กำหนด

1.4 การจัดการผู้ให้บริการภายนอก (Third Party Management)

(1) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องรับผิดชอบ(Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษา/ความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แม้ว่าผู้ให้บริการภายนอกจะการดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญขององค์กร

(2) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก โดยต้องควรคำนึงถึงสิ่งต่อไปนี้

(ก) ประเภทของผู้ให้บริการภายนอกที่สามารถเข้าถึงทรัพย์สินของบริการที่สำคัญโดยประเมินจากความต้องการทางธุรกิจขององค์กรและโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(ข) หน้าที่ความรับผิดชอบของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญขององค์กรจากภัยคุกคามทางไซเบอร์

(ค) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์ของผู้ให้บริการภายนอก

(ง) สิทธิ์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (ผู้ว่าจ้าง) ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

(3) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรกำหนดกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สาม และการตรวจสอบผลิตภัณฑ์ และควรติดตามการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

(4) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรพิจารณาดำเนินเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้เป็นสอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่ ๆ

2. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

2.1 การควบคุมการเข้าถึง (Access Control)

(1) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึงระบบข้อมูล และทรัพย์สินสารสนเทศที่เกี่ยวข้องกับบริการที่สำคัญ อย่างน้อยในเรื่องดังต่อไปนี้

(ก) กำหนดนโยบายการเข้าถึงหรือเข้าใช้งานระบบ ข้อมูล ทรัพย์สินด้านเทคโนโลยีสารสนเทศ รวมถึงนโยบายการใช้บริการเครือข่ายสื่อสารขององค์กร สอดคล้องตามข้อกำหนดการดำเนินธุรกิจ

(ข) กำหนดให้มีการบริหารจัดการสิทธิการใช้งาน และตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้ โดยคำนึงถึงความจำเป็นในการใช้งานและระดับความเสี่ยง

(ค) กำหนดให้มีการทบทวนปรับปรุงสิทธิการใช้งาน ตามรอบระยะเวลาที่กำหนด

(ง) กำหนดให้มีการเพิกถอนสิทธิการใช้งานเมื่อมีการเปลี่ยนแปลงหน้าที่งานหรือสิ้นสุดสภาพการเป็นพนักงาน หรือสิ้นสุดสัญญาการให้บริการภายนอกทันที

(2) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดให้แต่ละบุคลากร กิจกรรม และกระบวนการที่ได้รับอนุญาตให้เข้าใช้งานระบบหรือข้อมูล มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ

(3) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญ และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ โดยการกำหนดความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว รวมถึงความเสี่ยงของแต่ละบันทึก (Log)

(4) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องตรวจสอบและกำหนดให้การเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดย

(ก) การเชื่อมต่อปฏิบัติภายใต้การดูแลของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ข) ดำเนินการในสถานที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (หากเป็นไปได้)

2.2 การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

(1) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการแอปพลิเคชั่นและอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญขององค์กร ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญ

(2) มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) จะกล่าวถึงหลักการรักษาความมั่นคงปลอดภัย อย่างน้อยดังต่อไปนี้

(ก) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

(ข) การแบ่งแยกหน้าที่ (Separation of Duties)

(ค) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

(ง) การลบบัญชีที่ไม่ได้ใช้

(จ) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

(ฉ) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

(ช) การป้องกันมัลแวร์ (Malware) และ

(ซ) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

(3) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องตรวจสอบการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ก่อนที่จะมีทรัพย์สินใดๆ เชื่อมต่อ หรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(4) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องทบทวนมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

(5) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่อสามารถตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ

2.3 การเชื่อมต่อระยะไกล (Remote Connection)

(1) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดมาตรการควบคุมและจำกัดสิทธิการเข้าถึงระบบเครือข่าย และระบบสารสนเทศจากระยะไกล (Remote Access) โดยให้มีการควบคุมความปลอดภัยในการเชื่อมต่อระบบเครือข่ายจากภายนอก เพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

(2) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดมาตรการสำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญและต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

(ก) เปิดใช้งานการเชื่อมต่อไปยังหรือจากไซต์ระยะไกลเมื่อจำเป็นเท่านั้น

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

(ค) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

(ง) มีการรักษาความมั่นคงปลอดภัยของระบบที่สำคัญภายในองค์กรและระบบเครือข่ายที่มีการเชื่อมต่อหรือรับส่งข้อมูลที่เป็นความลับหรือมีความสำคัญจากระยะไกล เช่น การติดตั้ง Firewall การ Update โปรแกรมเพื่อป้องกัน Malware และการเข้ารหัสข้อมูล หรือเข้ารหัสระบบเครือข่าย เป็นต้น

(จ) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญเว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการทางธุรกิจ และ

(ฉ) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่มีการเชื่อมต่อเมื่อจำเป็นเท่านั้น

2.4 สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

(1) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดมาตรการการควบคุมอย่างเข้มงวดในการเชื่อมต่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญ โดยใช้มาตรการอย่างน้อย ดังนี้

(ก) ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อได้รับอนุญาตเท่านั้น

(ข) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตให้ใช้งานแล้วเท่านั้น

(ค) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญ

(2) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้

2.5 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

(1) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดแผนปฏิบัติงานและจัดให้มีการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงานผู้รับเหมาและผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ อย่างน้อยดังต่อไปนี้

(ก) จัดกิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่

- พนักงานใหม่ (New Employees)
- ผู้ใช้งานทั่วไปและผู้ใช้งานระดับผู้บริหาร (Users and Management)
- เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ผู้ให้บริการ IT และ ICS
- ผู้ขายผู้รับเหมาและผู้ให้บริการ (Vendors, Contractors and Service Providers)

(ข) การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ

(ค) สร้างความตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎระเบียบนโยบาย แนวปฏิบัติมาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ง) สื่อสารเกี่ยวกับภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบอย่างสม่ำเสมอและทันท่วงที

(จ) จัดให้มีการทดสอบความเข้าใจ และความตระหนักรู้ เพื่อให้แน่ใจว่าการสื่อสารและการจัดกิจกรรมต่างๆ บรรลุวัตถุประสงค์

(2) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องทบทวนแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

(3) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรกำหนดตัวชี้วัดการสร้างความตระหนักรู้ติดตามผลการดำเนินการตามตัวชี้วัดที่ตั้งไว้ และให้มีการจัดเก็บหลักฐานประกอบการติดตามผลดังกล่าว

2.6 การแบ่งปันข้อมูล (Information Sharing)

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูล เกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบหรืออาจเกิดขึ้นได้ ได้รับผลกระทบจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์หรือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ (เช่น ผู้ใช้ ผู้รับเหมาที่ให้บริการแก่บริการที่สำคัญ และเจ้าของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญ)

เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้ โดยรายละเอียด แนวทางและรูปแบบในการแบ่งปันให้เป็นไปตามหลักเกณฑ์และวิธีการที่ สกมช. กำหนด

3. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

3.1 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซบอร์ (Cyber Threat Detection and Monitoring)

(1) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดกลไกและกระบวนการที่เกี่ยวข้องกับการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ ดังต่อไปนี้

(ก) การตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญ

(ข) การจัดประเภทและการวิเคราะห์ระดับของเหตุการณ์ ผลกระทบที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

(ค) การระบุภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญ

(ง) การติดตาม การแก้ไขเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และการรายงานผลการติดตามไปยังผู้บริหารให้รับทราบอย่างสม่ำเสมอ

(2) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องดำเนินการทบทวนมาตรการและกระบวนการอย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพอยู่เสมอ

4. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

4.1 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

(1) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องมีการจัดทำและสื่อสาร แผนการรับมือภัยคุกคามไซเบอร์ให้ผู้ที่เกี่ยวข้องรับทราบ

(2) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องฝึกซ้อมแผนการรับมือภัยคุกคามไซเบอร์ที่กำหนดขึ้นอย่างน้อยปีละ 1 ครั้ง

(3) หลังจากการฝึกซ้อมแผนการรับมือภัยคุกคามไซเบอร์แล้วเสร็จ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องทบทวน และปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

4.2 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

(1) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(2) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต ประกอบด้วยอย่างน้อยดังต่อไปนี้

(ก) ทีมงาน การสื่อสาร และขั้นตอนการเปิดใช้งานในช่วงวิกฤต

(ข) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

(ค) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

(ง) ระบุบุคลากรซึ่งทำหน้าที่เป็นผู้สื่อสารกับหน่วยงานภายนอกและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน

(จ) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล และแจ้งข้อมูลต่างๆ ให้บุคลากรภายในและภายนอกรับทราบ

(3) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องสื่อสารแผนการสื่อสารในภาวะวิกฤตให้ผู้ที่เกี่ยวข้องรับทราบ เพื่อให้แน่ใจว่าทุกฝ่ายที่เกี่ยวข้องมีการตอบสนองที่ประสานและสอดคล้องกันในช่วงวิกฤต

(4) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ 1 ครั้งและให้มีการทบทวนแผนการสื่อสารดังกล่าวให้เหมาะสมกับสภาวการณ์เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

4.3 การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

(1) หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำการร่วมฝึกซ้อมด้านความมั่นคงปลอดภัยไซเบอร์โดยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดเตรียมบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามไซเบอร์ และเข้าร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

(2) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องปฏิบัติตามคำขอใด ๆ ของ กมช. เพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ โดยข้อมูลที่ กมช. อาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤตที่กำหนดขึ้นและขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญขององค์กร

5. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์(Cybersecurity Resilience and Recovery)

(1) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ตามหลักเกณฑ์และวิธีการที่ สกมช. กำหนดขึ้น เพื่อให้แน่ใจว่าบริการที่สำคัญสามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนขององค์กรเช่นความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ: Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

(2) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดให้มีการฝึกซ้อม BCP อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์

(3) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องวิเคราะห์ ทบทวนปรับปรุง BCP ดังกล่าว รวมถึงจัดเก็บผล การฝึกซ้อมแผน เพื่อให้แน่ใจว่า BCP ดังกล่าวรองรับต่อภัยคุกคามไซเบอร์เมื่อเกิดเหตุการณ์ได้ทันท่วงที

2. กลไกหรือขั้นตอนการเฝ้าระวังภัยคุกคามไซเบอร์

จากการศึกษามาตรฐานสากลต่างๆ เช่น NIST Security Framework ,ISO/IEC27001 และมาตรฐานอื่น ๆ ที่เกี่ยวข้อง จึงขอเสนอกลไกหรือขั้นตอนการเฝ้าระวังภัยคุกคามไซเบอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดังต่อไปนี้

แนวปฏิบัติขั้นพื้นฐานสำหรับการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

2.1.หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องมีการเตรียมการรับมือและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (Preparation) โดยจะต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้

(1) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดขั้นตอน กระบวนการ ทรัพยากร และอุปกรณ์สำหรับการติดต่อสื่อสารของบุคคลหรือองค์กรต่างๆ เพื่อรับมือภัยคุกคามทางไซเบอร์

(2) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดเตรียมข้อมูลสนับสนุนที่จำเป็นสำหรับการวิเคราะห์เหตุจากภัยคุกคามทางไซเบอร์ เช่น รายการทรัพย์สินสำคัญทางสารสนเทศ แผนผังโครงสร้างหรือเครือข่าย (Network Diagrams) เป็นต้น

(3) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรติดตั้งอุปกรณ์เพื่อตรวจจับและปิดกั้นการโจมตีหรือการบุกรุกโดยไม่อนุญาต ได้แก่ Intrusion Detection หรือ Prevention System (IDS/IPS)

(4) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรดำเนินการตรวจหาช่องโหว่ และเจาะระบบสำหรับอุปกรณ์ หรือระบบที่มีความเสี่ยงช่องโหว่ โดยให้มีการกำหนดรอบการตรวจหาช่องโหว่ และทดสอบเจาะระบบตามความเสี่ยงของแต่ละระบบอย่างสม่ำเสมอ

(5) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดมาตรการในการป้องกัน เฝ้าระวังและรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย อุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และระบบงาน โดยให้มีการตั้งค่าระบบงานให้มีความมั่นคงปลอดภัย การบริหารจัดการสิทธิในการเข้าถึงระบบงาน การรักษาความมั่นคงปลอดภัยของข้อมูล การพัฒนาระบบงาน ที่คำนึงถึงความปลอดภัยตามขั้นตอนหรือกระบวนการในการพัฒนาระบบงาน และการบริหารจัดการ Patch เป็นต้น

(6) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดมาตรการ ขั้นตอนปฏิบัติสำหรับการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ และจัดทำแผนการบริหารจัดการการ ตั้งค่าหรือการเปลี่ยนแปลงค่าของอุปกรณ์ (Configuration Management Plan)

(7) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรประเมินความเสี่ยงเกี่ยวกับการวิเคราะห์ความสำคัญของทรัพย์สินสำคัญทางสารสนเทศสำหรับการให้บริการ เช่น การวิเคราะห์ค่าวิกฤติของระบบงานต่าง ๆ ที่เกี่ยวข้องกับการให้บริการขององค์กร เป็นต้น

2. 2 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องมีการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detection) โดยจะต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้

(1) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดหน่วยงานที่รับผิดชอบในการติดตาม ดูแล เฝ้าระวัง วิเคราะห์ ประสานงาน และเป็นศูนย์กลางในการรับแจ้งและจัดการเหตุการณ์ผิดปกติทางไซเบอร์

(2) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรมีมาตรการแจ้งเตือนเมื่อพบเหตุการณ์ที่มีโอกาสเป็นการโจมตีทางไซเบอร์ เช่น Log Event Alert เป็นต้น รวมถึงมีเครื่องมือตรวจจับเหตุการณ์ผิดปกติ

(Incident) และกระบวนการในการตรวจจับและแจ้งเตือนเมื่อตรวจพบพฤติกรรมหรือเหตุการณ์ที่ผิดปกติ หรือการพยายามบุกรุกเครือข่ายที่อาจจะสร้างความเสียหายต่อบริษัท

(3) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องมีการจัดเก็บบันทึกเหตุการณ์ (Logs) โดยบันทึกเหตุการณ์ดังกล่าวอย่างน้อย 90 วัน หรือตามกฎหมายที่เกี่ยวข้องกำหนดด้วยวิธีการที่ปลอดภัยโดยต้องบันทึกเหตุการณ์ อย่างน้อยดังต่อไปนี้

- บันทึกการเข้าถึง (Access Log)
- บันทึกการดำเนินงาน (Activity Log) ที่สำคัญ
- บันทึกร่องรอยกิจกรรมการทำธุรกรรมต่างๆ (Transaction Log)
- บันทึกด้านการรักษาความปลอดภัย (Security Event Log)

(4) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรมีกระบวนการวิเคราะห์ข้อมูลและประวัติการใช้งานต่างๆ เช่นลักษณะการใช้งานเครือข่ายและระบบงานเป็นต้น รวมถึงสอบทาน Logs ของผู้ปฏิบัติที่มีสิทธิสูงอย่างสม่ำเสมอ เช่น System Administrator, System Operator เป็นต้น

(5) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรมีการแจ้งเตือนได้ทันที (Real-time Alerts) เมื่อพบภัยคุกคามทางไซเบอร์เพื่อให้มีการตอบสนองที่ทันท่วงที

(6) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดช่องทางในการรายงานช่องโหว่ จุดอ่อน เหตุการณ์ หรือสถานการณ์ที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ให้ผู้ที่เกี่ยวข้องทั้งภายในและภายนอก รวมถึงรายงานการถูกคุกคามทางไซเบอร์และกิจกรรมต้องสงสัย โดยหากตรวจพบเหตุการณ์ผิดปกติที่อาจจะส่งผลให้การบริการ ที่สำคัญหยุดชะงัก หรือส่งผลต่อผู้ใช้บริการในวงกว้าง ต้องรีบแจ้งให้สำนักงาน กสทช. รับทราบเหตุผิดปกติดังกล่าวทันที

(7) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรวิเคราะห์ข้อมูลของภัยคุกคามทางไซเบอร์ที่เกิดขึ้น และค้นหาความสัมพันธ์ของข้อมูลกับเหตุการณ์ต่างๆ เพื่อเพิ่มความสามารถในการรับรู้และดำเนินการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

2. 3 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องมีมาตรการในการรับมือและตอบสนองเมื่อตรวจพบภัยคุกคามทางไซเบอร์ (Response) โดยจะต้องมีการดำเนินการอย่างน้อยดังต่อไปนี้

(1) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรกำหนดแนวทางการบริหารจัดการ วางแผน มาตรฐานและระเบียบ วิธีปฏิบัติในการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติหรือภัยคุกคามทางไซเบอร์ ซึ่งรวมถึงการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (Digital Forensics) อย่างชัดเจนและมีแผนการดำเนินธุรกิจอย่างต่อเนื่อง เพื่อตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์

(2) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรจัดให้มีการจัดทำแนวการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ โดยให้มีการตรวจสอบ วิเคราะห์หาสาเหตุ และประเมินผลกระทบเพื่อให้สามารถใช้อ้างอิงในการรับมือภัยคุกคาม ตอบสนองต่อเหตุการณ์ และกู้คืนระบบและข้อมูลได้อย่างรวดเร็วและทันท่วงที

(3) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรกำหนดช่องทางและวิธีการสื่อสารและส่งต่อข้อมูลการปฏิบัติงาน หากเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ไปยังผู้ที่เกี่ยวข้อง เพื่อให้ผู้ที่เกี่ยวข้องทราบถึงขั้นตอนการปฏิบัติงาน และรายงานข้อมูลเหตุการณ์ทางไซเบอร์ทันการณ์

(4) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรกำหนดวิธีการ ช่องทางในการแจ้งผู้เกี่ยวข้องทั้งภายใน และภายนอก ซึ่งได้แก่ลูกค้า สำนักงาน กสทช. และหน่วยงานที่บังคับใช้กฎหมายทราบเมื่อเกิดเหตุการณ์ผิดปกติทางไซเบอร์

(5) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรจัดให้มีการทดสอบแผนฉุกเฉินในการรับมือภัยคุกคามทางไซเบอร์ และระบบงานสำคัญ

(6) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรจัดทำรายงานสรุปการทดสอบแผนฉุกเฉินในการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ต่อคณะกรรมการหรือผู้มีอำนาจบริหารของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ