แผนรับมือเหตุภัยคุกคามทางไซเบอร์
ของสำนักงานเศรษฐกิจการคลัง

ศูนย์เทคโนโลยีสารสนเทศ
สำนักงานเศรษฐกิจการคลัง

รายละเอียดการบังคับใช้เอกสาร

รายละเอียดของเอกสาร (Document control and review)

รายละเอียดของเอกสาร (Document control)	
ผู้จัดทำเอกสาร (Author)	ส่วนนโยบายโครงสร้างพื้นฐานและความมั่นคงปลอดภัย
ผู้ดำเนินการตามเอกสาร (Owner)	หน่วยงานภายในสำนักงานเศรษฐกิจการคลังและหน่วยงานภายนอกที่เกี่ยวข้อง
วันที่จัดทำเอกสาร (Date created)	วันที่ ๒๕๖๘
ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by)	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ สำนักงานเศรษฐกิจการคลัง
วันที่ตรวจสอบความถูกต้องของเอกสาร (Last date reviewed)	วันที่ ๒๕๖๘
ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date)	ผู้อำนวยการสำนักงานเศรษฐกิจการคลัง
วันที่จะต้องมีการตรวจสอบเอกสารครั้งถัดไป (Next review due date)	

การเปลี่ยนแปลงเอกสาร (Version control)

รุ่น (Version)	วันที่อนุมัติ (Date of Approval)	ผู้อนุมัติ (Approved by)	สถานะ (Description of change)
๑	วันที่ ๒๕๖๘		

สารบัญ

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานเศรษฐกิจการคลัง

๑. หลักการและเหตุผล

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานเศรษฐกิจการคลังฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วย (๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง และ (๒) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของสำนักงานเศรษฐกิจการคลังด้วย

๒. วัตถุประสงค์

เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในสำนักงานเศรษฐกิจการคลัง โดยจะเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับกอง/ศูนย์/กลุ่ม ต่าง ๆ ภายใต้สำนักงานเศรษฐกิจการคลัง การกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสียเพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของสำนักงานเศรษฐกิจการคลัง

๓. ขอบเขต

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานเศรษฐกิจการคลังจะเป็นการกำหนดโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ บทบาทหน้าที่ความรับผิดชอบ และโครงสร้างการรายงานเหตุการณ์ รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ รวมถึงข้อมูลดิจิทัลของสำนักงานเศรษฐกิจการคลัง ตลอดจนบุคคลหรืออุปกรณ์ใด ๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

๔. หน้าที่การทบทวนแผน

ศูนย์เทคโนโลยีสารสนเทศ สำนักงานเศรษฐกิจการคลัง มีหน้าที่จัดทำและทบทวนแผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานเศรษฐกิจการคลัง โดยจัดให้มีการทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีเหตุการณ์สำคัญ

/๕. หน้าที่ ...

๕. หน้าที่ในการดำเนินการตามแผน

ส่วนนโยบายโครงสร้างพื้นฐานและความมั่นคงปลอดภัย ศูนย์เทคโนโลยีสารสนเทศ มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานเศรษฐกิจการคลัง โดยมีหน่วยงานสนับสนุนประกอบด้วย ศูนย์เทคโนโลยีสารสนเทศ และ กอง/ศูนย์/กลุ่ม ที่เป็นเจ้าของกระบวนการที่เกี่ยวข้องหรือเจ้าของข้อมูลภายในสำนักงานเศรษฐกิจการคลัง

๖. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

๖.๑ นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้อง

- นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๑
- แผนบริหารความเสี่ยงต่อทรัพยากรเทคโนโลยีสารสนเทศและเครือข่ายของสำนักงานเศรษฐกิจการคลัง เพื่อบริหารจัดการกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO
- แผนบริหารความต่อเนื่องในสภาวะวิกฤตของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๕
- แผนบริหารจัดการความเสี่ยงของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๖

๖.๒ นโยบายและแนวปฏิบัติด้านการปกป้องข้อมูลส่วนบุคคลที่เกี่ยวข้อง

นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๗

๖.๓ กฎหมายที่เกี่ยวข้อง

ที่	กฎหมายที่เกี่ยวข้อง
๑	**พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม**
	ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๖๔
๒	**พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒**
	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา ๔๑ (๒) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๖

/กฎหมายที่เกี่ยวข้อง ...

ที่	กฎหมายที่เกี่ยวข้อง
๓	**พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒**
	ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔
	ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔
	ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖
	ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖
	ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

๗. นิยาม

เหตุการณ์ (Event) หมายความว่า เหตุการณ์ที่เกิดขึ้นจากการเฝ้าระวังสังเกตการณ์ (observable occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

เหตุภัยคุกคามทางไซเบอร์ (Cyber incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

/๘. บทบาท ...

๘. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

๘.๑ ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

ลำดับ	ชื่อ – นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	นายสุขุมภัทร จุฬุวรรณ	เวลาทำการ จ. - ศ. เวลา ๘.๓๐ น. – ๑๖.๓๐ น. และกรณีฉุกเฉินนอกเวลาทำการ	๐๘๕-๔๕๐-๒๓๓๐	รับแจ้งเหตุ	เป็นผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ และบันทึกเหตุการณ์ พร้อมทั้งรายงานให้หัวหน้าทีมรับมือทราบ รวมถึงตรวจสอบ ติดตามเจ้าหน้าที่บริษัทคู่สัญญา
๒	นายปิยวรรษ เกียรติกูล	เวลาทำการ จ. - ศ. เวลา ๘.๓๐ น. – ๑๖.๓๐ น. และกรณีฉุกเฉินนอกเวลาทำการ	๐๖๑-๔๔๖-๒๖๔๔	รับแจ้งเหตุ	เป็นผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ และบันทึกเหตุการณ์ พร้อมทั้งรายงานให้หัวหน้าทีมรับมือทราบ รวมถึงตรวจสอบ ติดตามเจ้าหน้าที่บริษัทคู่สัญญา
๓	เจ้าหน้าที่บริษัทคู่สัญญา	ตลอดระยะเวลา ๒๔ ชั่วโมง / ๗ วัน	มือถือ	เจ้าหน้าที่บริษัทคู่สัญญา	ตรวจสอบแก้ไขและรายงานผลการดำเนินงาน

๘.๒ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

สำนักงานเศรษฐกิจการคลัง ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (ทีมรับมือ) ในลักษณะแบบรวมศูนย์ ประกอบด้วย

ลำดับ	ชื่อ - นามสกุล รายละเอียดการติดต่อ	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	นายสุภชัย ภูริเกษม ผู้อำนวยการ ศูนย์เทคโนโลยีสารสนเทศ	๐๘๖-๙๙๙-๙๙๖๖	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน

/ลำดับ ...

ลำดับ	ชื่อ - นามสกุล รายละเอียดการติดต่อ	ช่องทางการ ติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๒	นายนิติสิริ ประสาทกุล ผู้อำนวยการส่วนระบบข้อมูลและนวัตกรรมเทคโนโลยีสารสนเทศ	๐๘๑-๖๒๖-๓๐๔๖	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่ หรือไม่สามารถปฏิบัติงานได้
๓	นายสุขุมภัทร จุฬุวรรณ	๐๘๕-๔๕๐-๒๓๓๐	เจ้าหน้าที่เทคนิค (Technical lead)	ทำหน้าที่ให้ความช่วยเหลือ ติดตาม ตรวจสอบระบบสารสนเทศและระบบเครือข่าย พร้อมทั้งให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๔	นายปิยวรรษ เกียรติกูล	๐๖๑-๔๔๖-๒๖๔๔	เจ้าหน้าที่เทคนิค (Technical lead)	ทำหน้าที่ให้ความช่วยเหลือ ติดตาม ตรวจสอบระบบสารสนเทศและระบบเครือข่าย พร้อมทั้งให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๕	เจ้าหน้าที่บริษัท คู่สัญญาที่ดูแลการโจมตีทางไซเบอร์		เจ้าหน้าที่บริษัท คู่สัญญาที่ดูแลการโจมตีทางไซเบอร์	ดำเนินการแก้ไขเหตุขัดข้องตามสัญญาที่ตกลงกันไว้ร่วมกัน
๖	เจ้าหน้าที่บริษัท คู่สัญญาที่ดูแลระบบสารสนเทศ		เจ้าหน้าที่บริษัท คู่สัญญาที่ดูแลระบบสารสนเทศที่เกี่ยวข้อง	ดำเนินการแก้ไข/กู้คืนระบบสารสนเทศตามสัญญาที่ตกลงกันไว้ร่วมกัน

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานเศรษฐกิจการคลัง (สศค.) (แผนรับมือฯ) ดังนี้

ลำดับ	บุคลากรที่เกี่ยวข้อง	หน้าที่	ความรับผิดชอบ
๑	ผอ. กอง/สำนัก	เจ้าหน้าที่บริหารจัดการผลกระทบจากภัยคุกคามทางไซเบอร์	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๒	นิติกร สศค.	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ทำหน้าที่ตรวจสอบแผนรับมือฯ ให้สอดคล้องกับกฎหมายที่เกี่ยวข้อง

/ลำดับ ...

ลำดับ	บุคลากรที่เกี่ยวข้อง	หน้าที่	ความรับผิดชอบ
๓	เจ้าหน้าที่บริษัทคู่สัญญา	ผู้ทดสอบเจาะระบบ	ทำหน้าที่ตาม [นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของ]
๔	ผู้เชี่ยวชาญด้านกฎหมาย	ผู้เชี่ยวชาญด้านกฎหมาย	ทำหน้าที่เป็นที่ปรึกษาด้านกฎหมายที่เกี่ยวข้อง
๕	เจ้าหน้าที่ ศทส. ที่ได้รับมอบหมาย	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ตาม [นโยบาย หรือคำสั่งที่เกี่ยวข้องของหน่วยงาน]
๖	เจ้าหน้าที่ ศทส. ที่ได้รับมอบหมาย	ผู้รับผิดชอบด้านสื่อสารองค์กร	ทำหน้าที่ตาม [นโยบาย หรือคำสั่งที่เกี่ยวข้อง]

๘.๓ <u>หน่วยงานภายนอกที่เกี่ยวข้อง</u>

ข้อมูลติดต่อสื่อสารของหน่วยงานภายนอกที่เกี่ยวข้อง เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.), หน่วยงานกำกับดูแล (Regulator), THAI – CERT และผู้ให้บริการภายนอกของ สศค. เป็นต้น

ลำดับที่	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
๑	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	โทร ๐๒-๑๔๒-๖๘๘๘	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	แจ้งเหตุภัยคุกคามทางไซเบอร์ และให้คำแนะนำ/แนวทางการรับมือภัยคุกคามทางไซเบอร์
๒	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ Thailand Computer Emergency Response Team (ThaiCERT)	โทร ๐๒-๑๔๒-๖๘๘๘ Email: thaicert@ncsa.or.th	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ Thailand Computer Emergency Response Team (ThaiCERT)	แจ้งเหตุภัยคุกคามทางไซเบอร์
๓	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	โทร ๐๒-๑๔๒-๑๐๓๓ โทร ๐๒-๑๔๑-๖๙๙๓	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุละเมิดข้อมูลส่วนบุคคล

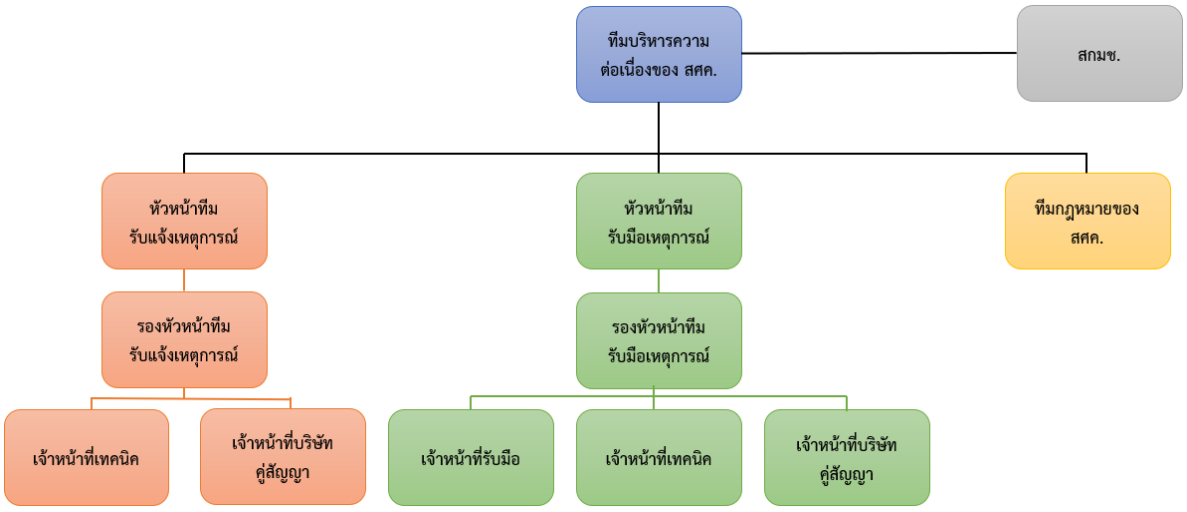
/ลำดับที่ ...

ลำดับที่	ชื่อ - นามสกุล	ช่อง ทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
๔	บริษัทคู่สัญญา ดูแลระบบ Network		บริษัทผู้ให้บริการภายนอก	ดูแลระบบ Network
๕	บริษัทคู่สัญญา ดูแลระบบ VM		บริษัทผู้ให้บริการภายนอก	ดูแลระบบ VM
๖	บริษัทคู่สัญญา ดูแลระบบ Backup		บริษัทผู้ให้บริการภายนอก	ดูแลระบบ Backup
๗	บริษัทคู่สัญญา ดูแลระบบ Data Center		บริษัทผู้ให้บริการภายนอก	ดูแลระบบ Data Center
๘	บริษัทคู่สัญญา ดูแลระบบ Storage		บริษัทผู้ให้บริการภายนอก	ดูแลระบบ Storage
๙	บริษัทคู่สัญญา ดูแลระบบตรวจจับและป้องกันมัลแวร์		บริษัทผู้ให้บริการภายนอก	ดูแลระบบตรวจจับและป้องกันมัลแวร์k

๘.๔ <u>โครงสร้างการรายงานเหตุการณ์</u> (Incident Reporting Structure)

สำนักงานเศรษฐกิจการคลังได้จัดให้มีแผนผังโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ของบุคลากรภายในทีมรับมือฯ ผู้บริหารหน่วยงาน หน่วยงานกำกับดูแล หน่วยงานรับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ตามกฎหมาย และหน่วยงานภายนอก เป็นต้น รวมถึงกำหนดว่า หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติและกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมายและข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดังรูป

/รูปที่ ๑ โครงสร้าง ...



รูปที่ ๑ โครงสร้างการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
(Incident Reporting Structure)

๙. รูปแบบภัยคุกคามไซเบอร์

๙.๑ Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูล ไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึงไวรัส (Virus) เวิร์ม (worms) โทรจัน (Trojans)

๙.๒ Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้วจะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

๙.๓ Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่าง ๆ เช่น E-Mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

๙.๔ Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น Code ของเว็บไซต์และ Web Server หรือ Database Server

๙.๕ Spam คือ วิธีการที่ผู้ส่งหรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล ข้อความหรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์หรือช่องทาง Social โดยเป็นการส่งจำนวนมากหรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญหรือก่อกวน

/๙.๖ DDoS ...

๙.๖ DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการหรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

๙.๗ Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ ข้อมูลของแอปพลิเคชันหรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชันหรือผู้ให้บริการระบบไม่ทราบซึ่งผู้โจมตีต้องการนำข้อมูลไปขายหรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ

๙.๘ Insider threat คือ ภัยที่เกิดจากบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ขององค์กร หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กรอาจจะมีการป้องกันในระดับต่ำทำให้เกิดการโจมตีประเภทนี้ได้ง่ายและเสี่ยงต่อข้อมูลสำคัญที่อาจจะถูกขโมย ซึ่งผลลัพธ์ของภัยนี้มีความรุนแรงต่อภาพลักษณ์องค์กรและการขาดความน่าเชื่อถือ

๙.๙ Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดีที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๙.๑๐ Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่องทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

๙.๑๑ Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่าง ๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไปที่ Hacker

๙.๑๒ ผู้บุกรุก (Hacker) ผู้ที่ไม่ได้รับอนุญาตให้เข้าใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหายจากผู้บุกรุกเป็นภัยคุกคามที่หนัก

๑๐. ขั้นตอนการรับมือกับภัยคุกคามทางไซเบอร์

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานเศรษฐกิจการคลังฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ

/และหน่วยงาน ...

และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ โดยมีขั้นตอนการดำเนินการ เป็น ๔ ขั้นตอนหลัก เพื่อให้สอดคล้องกับมาตรฐานหรือแนวทางปฏิบัติที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ ดังนี้

รูปที่ ๒ ภาพแสดงขั้นตอนการดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์ (Incident Handling Cycle)

๑๐.๑ ขั้นการเตรียมการ (preparation)

การดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งจำเป็นที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดตามข้อ ๘.๒

(๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) รายละเอียดตามข้อ ๘.๔

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และ CIRT

- การจัดเตรียมข้อมูลและอุปกรณ์ให้พร้อมต้องจัดเตรียมทรัพยากรและเครื่องมือที่จำเป็นต่อการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์
- การตั้งค่าอุปกรณ์และระบบต่าง ๆ ให้มีความปลอดภัยและเหมาะสม
- การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือแนวทางป้องกันและการเตรียมการเบื้องต้น

/(๔) จัดเตรียม ...

(๔) จัดเตรียมข้อมูลและอุปกรณ์ในการสื่อสารของบุคลากรผู้ทำหน้าที่รับมือและตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ ได้แก่

- รายชื่อและช่องทางการติดต่อของผู้ที่เกี่ยวข้องและประสานงานในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ รายละเอียดตามข้อ ๘.๒
- ช่องทางการรายงานเหตุการณ์ให้ผู้ได้รับผลกระทบหรือพบเห็นเหตุการณ์แจ้งศูนย์เทคโนโลยีสารสนเทศตรวจสอบ
- ช่องทางรายงานและติดตามข้อมูล สถานการณ์การดำเนินการของเหตุการณ์ที่ได้รับแจ้ง

(๕) จัดเตรียมอุปกรณ์ ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ ได้แก่

- จัดเตรียมสถานที่จัดเก็บที่มีความมั่นคงปลอดภัย เพื่อใช้ในการจัดเก็บหลักฐาน ข้อมูล และพยานวัตถุอื่น ๆ ที่สำคัญ
- ดำเนินการตั้งค่าระบบต่าง ๆ ให้ปลอดภัย เป็นการตั้งค่าอุปกรณ์เครือข่ายที่จำเป็น เช่น Firewall IPS เป็นต้น การกำหนดแนวทางการรักษาความมั่นคงปลอดภัยของห้องปฏิบัติการศูนย์ข้อมูล มีการปิดช่องโหว่และการกำหนดสิทธิ์ของผู้ใช้โดยการให้สิทธิ์เท่าที่จำเป็นต่อการปฏิบัติงานที่ได้รับอนุญาตเท่านั้น การ Update Security Patch เป็นประจำ การมี Software ในการป้องกันและตรวจจับความผิดปกติในระบบ เช่น Malware Prevention

(๖) จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Risk Assessment)

(๗) จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ของหน่วยงาน (รายละเอียดปรากฏตามภาคผนวก ๑)

นอกจากนี้ สำนักงานเศรษฐกิจการคลังยังดำเนินการตามแนวปฏิบัติพื้นฐาน (Security Control Baselines) เพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (รายละเอียดปรากฏตามภาคผนวก ๒)

/๑๐.๒ ขั้นการตรวจจับ ...

๑๐.๒ ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

เป็นการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้สามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงที เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น มีมาตรการและแนวปฏิบัติตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ประกาศ กมช. เรื่อง ลักษณะภัยคุกคามฯ) โดยดำเนินการดังต่อไปนี้

(๑) ทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ดำเนินการจัดเตรียมแนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้นหรืออาจเกิด (Common Attack Vectors/Common Threat Vectors) โดยการโจมตีรูปแบบทั่วไปที่อาจเกิดขึ้น ดังนี้

ประเภทภัยคุกคามของหน่วยงาน	คำอธิบาย	วิธีการรับมือ
อุปกรณ์แบบถอดได้ (External/Removable Media)	การโจมตีที่ดำเนินการจากอุปกรณ์แบบถอดได้หรืออุปกรณ์ต่อพ่วง เช่น โค้ดที่เป็นอันตรายแพร่กระจายไปยังระบบจากแฟลชไดรฟ์ที่ติดไวรัส	ดำเนินการถอนการติดตั้งอุปกรณ์แบบถอดได้ที่เป็นสาเหตุของภัยคุกคามออกจากอุปกรณ์และระบบเครือข่ายและตรวจสอบสาเหตุและประเภทของภัยคุกคามว่าเป็นภัยคุกคามประเภทใด
Website Defacement	การโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลที่เผยแพร่หน้าเว็บ ซึ่งผู้โจมตีมีวัตถุประสงค์เพื่อปรับเปลี่ยนหน้าเว็บไซต์แรกของเว็บไซต์เป้าหมาย หรือทั้งเว็บไซต์ จากเดิมไปเป็นหน้าเว็บไซต์ใหม่	ดำเนินการปิด DNS ขานอกที่เป็นสาเหตุของภัยคุกคาม จากนั้นผู้ดูแลระบบเว็บไซต์ดำเนินการลบไฟล์ที่น่าสงสัย
DDos	การโจมตี DDos เกิดขึ้นเมื่อ Hacker ส่งปริมาณการเข้าชมจำนวนมากไปยังเครือข่ายหรือเซิร์ฟเวอร์ เพื่อทำลายระบบและขัดขวางความสามารถในการให้บริการ การโจมตีเหล่านี้มักถูกนำมาใช้เพื่อโจมตีเว็บไซต์หรือแอปพลิเคชันให้ออฟไลน์ชั่วคราวและการโจมตีแต่ละครั้งอาจเกิดขึ้นเป็นระยะเวลาหลายวันหรือนานกว่านั้น	- ปิดกัน IP ต้องสงสัย - กำหนด Rate Limit ของ Connection
SQL Injection	การโจมตีที่ระบบฐานข้อมูลของเว็บไซต์ ผลคือระบบฐานข้อมูลจะถูกขโมยออกไป หรืออาจจะถูกลบ หรือแก้ไขให้เกิดความเสียหายได้ ช่องโหว่ของ SQL เป็นรูปแบบที่มีมานาน และถูกใช้เป็นจุดอ่อนที่ถูกโจมตีมากที่สุด ซึ่งจุดอ่อนนี้สามารถเกิดขึ้นได้กับระบบฐานข้อมูล เช่น Oracle, Microsoft, MySQL หรืออื่น ๆ	- ทำ Penetration Testing ทุกเว็บไซต์ - Monitor Traffic ต้องสงสัยผ่านระบบ SIEM และแจ้งผู้ดูแลเว็บไซต์เมื่อตรวจสอบพบการโจมตี

ประเภทภัยคุกคามของหน่วยงาน	คำอธิบาย	วิธีการรับมือ
การโจมตีในรูปแบบ Network Scanning	กระบวนการที่ผู้ไม่ประสงค์ดีพยายามทำลายหรือเข้าถึงข้อมูลในระบบเครือข่ายของบุคคลหรือองค์กรอย่างไม่ถูกต้องหรือไม่ได้รับอนุญาต โดยเครื่องมือที่ออกแบบมาเพื่อสแกนหรือสำรวจเครือข่าย	ตรวจสอบ Log ที่มาจาก Firewall, IPS, End Point
Malicious Code (โปรแกรมไม่พึงประสงค์)	มัลแวร์ (Malware), Virus, Worm, Trojan, Ransomware, และ Spyware ต่าง ๆ ซึ่งเป็นโปรแกรมที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์ เช่น การโจมตีในรูปแบบ Ransomware โดยการเข้ารหัสไฟล์ของเหยื่อแล้วขโมยข้อมูลของเหยื่อไป จากนั้นผู้โจมตีก็จะเรียกค่าไถ่จากเหยื่อ เพื่อให้เหยื่อยอมจ่ายเงินแลกกับการได้ข้อมูลคืน ช่องทางการโจมตีมาจาก File Attachment ที่แนบ e-Mail เช่น ไฟล์ PDF ที่แนบ Script Ransomware ทำให้เครื่องคอมพิวเตอร์ภายในถูก Ransomware โจมตีและแพร่กระจายไปยังเครื่องคอมพิวเตอร์ ภายในเครือข่ายเดียวกัน	- ทำการรวบรวม Log ทั้งหมดที่เกี่ยวข้องเพื่อทำการวินิจฉัยว่ามีเหตุการณ์ Scan ระบบเครือข่าย - ดำเนินการปิดการเชื่อมต่อ Port SMB* ของเครื่องคอมพิวเตอร์ที่เชื่อมโยงภายในเครือข่ายคอมพิวเตอร์เดียวกัน - ติดตั้งอุปกรณ์ป้องกันการถูกโจมตีจากภัยทางไซเบอร์บนเครือข่ายคอมพิวเตอร์ *Port SMB (Server Message Block) เป็นพอร์ตเครือข่ายที่ใช้สำหรับการแบ่งปันไฟล์และทรัพยากรบนเครือข่ายคคอมพิวเตอร์เป็นหลัก SMB ทำงานบนพอร์ต TCP ๔๔๕ และเปิดใช้งานการเข้าถึงไฟล์ เครื่องพิมพ์ และพอร์ตซีเรียลร่วมกันระหว่างอุปกรณ์บนเครือข่าย
หมวดหมู่ของภัยคุกคามทางไซเบอร์ (ตามประกาศ กมช. เรื่อง ลักษณะภัยคุกคามฯ)	**คำอธิบาย**	**วิธีการรับมือ**
หมวดหมู่ : ๑ การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)	การพยายามทำกิจกรรมที่ไม่สำเร็จ (เหตุการณ์) ความพยายามโดยเจตนาเพื่อเข้าถึงระบบโดยไม่ได้รับอนุญาต ซึ่งพ่ายแพ้โดยกลไกการป้องกันตามปกติ ผู้โจมตีไม่สามารถเข้าถึงระบบ (เช่น ผู้โจมตีพยายามใช้ชื่อผู้ใช้และรหัสผ่านที่ถูกต้องหรืออาจถูกต้อง) และกิจกรรมนี้ไม่สามารถจัดประเภทเป็นการสแกนเชิงสำรวจได้	ดำเนินการตรวจสอบจากการแจ้งเตือนจากอุปกรณ์ที่ตรวจจับสิ่งผิดปกติและทางเจ้าหน้าที่วิเคราะห์ภัยคุกคามจะต้องตรวจสอบ เพื่อให้แน่ใจว่าสิ่งที่แจ้งเตือนมานั้นเป็นเหตุการณ์ที่ต้องระงับและดำเนินการขั้นตอนให้ภัยคุกคามนั้นลดลงหรือหมดไป
หมวดหมู่ : ๒ การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	กิจกรรมที่พยายามรวบรวมข้อมูลที่ใช้เพื่อระบุลักษณะของระบบ แอปพลิเคชัน เครือข่าย ข้อมูล และผู้ใช้งานในระบบที่อาจมีประโยชน์ในการกำหนดการโจมตี	ดำเนินการบล็อก IP ต้นทาง และสร้าง Rule เพื่อบล็อกการ Scan ระบบเครือข่าย หลังจากนั้นให้ทำการรวบรวมหลักฐานของเหตุการณ์ Scan ระบบเครือข่ายเพื่อนำไปสร้างรายงานและองค์ความรู้

/หมวดหมู่ ...

หมวดหมู่ของภัยคุกคามทางไซเบอร์ (ตามประกาศ กมช. เรื่อง ลักษณะภัยคุกคามฯ)	คำอธิบาย	วิธีการรับมือ
หมวดหมู่ : ๓ การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)	ความเสี่ยงที่เกิดขึ้นกับระบบอาจมาจากการกระทำหรือการละเลยของผู้ใช้งานระบบ เช่น การละเลยการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด การไม่ติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น ซึ่งพฤติกรรมดังกล่าวส่งผลให้เกิดช่องโหว่ที่อาจนำไปสู่การโจมตีทางไซเบอร์ และเป็นต้นเหตุของความเสียหายต่อระบบและข้อมูลสำคัญ	สร้างความตระหนักรู้ให้กับผู้ใช้งานอย่างสม่ำเสมอ แสดงให้เห็นถึงความเสี่ยงของการไม่ดำเนินการตามมาตรฐานที่กำหนด
หมวดหมู่ : ๔ การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	เป็นเหตุการณ์ที่เครื่องคอมพิวเตอร์ลูกข่ายหรือเครื่องคอมพิวเตอร์แม่ข่ายถูกบุกรุกโดยการใช้มัลแวร์ (Malicious Logic) หรือชุดคำสั่งไม่พึงประสงค์ที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่ง	ดำเนินการตัดการเชื่อมต่อทางเครือข่ายและตรวจสอบ Log และใช้เครื่องมือกำจัดมัลแวร์
หมวดหมู่ : ๕ การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	การเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือข้อมูล/บัญชีที่ไม่ได้รับอนุญาต หรือมีสิทธิ์การเข้าถึงระบบที่เกินกว่าสิทธิ์การใช้งานที่ได้รับจากผู้ดูแลระบบ	ดำเนินการตรวจสอบ Log ที่มาจาก Firewall, IPS, End Point ว่าเป็นไปตามเกณฑ์ ต่อไปนี้ ๑. พยายาม Log-in นอกเวลางาน ๒. Log-in ภายใต้ IP ที่กำหนด
หมวดหมู่ : ๖ การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	การเข้าถึงระบบงานด้วยสิทธิพิเศษโดยไม่ได้รับอนุญาต การเข้าถึงแบบมีสิทธิพิเศษในระดับผู้ดูแลระบบหรือระดับ Root ช่วยให้เข้าถึงระบบงานได้ไม่จำกัด	ดำเนินการตรวจสอบ Log ที่มาจาก Firewall, IPS, End Point ว่าเป็นไปตามเกณฑ์ ต่อไปนี้ ๑. พยายาม Log-in นอกเวลางาน ๒. Log-in ภายใต้ IP ที่กำหนด

/(๒) การตรวจจับ ...

(๒) การตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลความรู้จากแหล่งข้อมูลข่าวสารภัยคุกคามจากภายนอกต่าง ๆ (Threat Intelligence) เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น จากหลากหลายช่องทางดังนี้

Channel Types	URL
Cybersecurity news sites	
	https://webboard-nsoc.ncsa.or.th/category/12/cyber-security -news
	https://www.thaicert.or.th/category/cybernews/
	https://www.blognone.com/
	https://www.techtalkthai.com/category/security/
	https://thehackernews.com
Community Facebook Pages	
	https://www.facebook.com/NCSA.Thailand/
	https://www.facebook.com/thaicert/
	https://www.facebook.com/pdpc.th/
	https://www.facebook.com/TBCERT.Official/
	https://www.facebook.com/2600Thailand/
	https://www.facebook.com/owaspbangkok/
	https://www.facebook.com/InfoSecThaiGirl/
	https://www.facebook.com/thaicysec/
	https://www.facebook.com/hackandsecbook/
	https://www.facebook.com/isecure.mssp/
Cyber Threat intelligence Tools	
	https://attack.mitre.org/
	https://www.talosintelligence.com/
	https://www.virustotal.com/gui/
	https://otx.alienvault.com/browse/
	https://urlscan.io
	https://www.opencve.io/cve
	https://www.cvedetails.com/
	https://www.filescan.io/scan
	https://dnsdumpster.com

/(๓) ทีมรับมือ ...

(๓) ทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ดำเนินการวิเคราะห์ผลกระทบ พร้อมทั้งระดับของภัยคุกคามทางไซเบอร์ (Incident Prioritization) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort) เป็นต้น

➢ **ระดับความรุนแรงของภัยคุกคามทางไซเบอร์ (Incident Prioritizaton) ดังนี้**

ระดับความรุนแรงของภัยคุกคามทางไซเบอร์ (Security Level)	คำอธิบาย	ประเภท/รูปแบบของภัยคุกคาม
๐ ระดับต่ำ (Low)	ภัยคุกคามทางไซเบอร์ที่ส่งผลต่อระบบคอมพิวเตอร์ อุปกรณ์ โครงสร้างเครือข่าย หรือระบบงานเพียงเล็กน้อย หรืออาจทำให้ด้อยประสิทธิภาพลงไปบ้าง แต่ไม่กระทบกับระบบโดยรวม	- ไวรัสคอมพิวเตอร์ (Computer Virus) - หนอนคอมพิวเตอร์ (Computer worm) - Spam Mail หรืออีเมล์ขยะ - Botnet - สปายแวร์ (Spyware)
๑ ระดับกลาง (Medium)	ภัยคุกคามทางไซเบอร์ที่ส่งผลต่อระบบคอมพิวเตอร์ อุปกรณ์ โครงสร้าง เครือข่าย หรือระบบงานเพียงเล็กน้อย หรืออาจทำให้ด้อยประสิทธิภาพลงไปบ้าง แต่ไม่ถึงกับทำให้ระบบหรือบริการต้องหยุดชะงัก หรือไม่สามารถใช้งานได้	- ม้าโทรจัน (Trojan horse) - Backdoor - Rootkit - การโจมตีแบบ DoS/DDoS - Phishing
๒ ระดับสูง (High)	ภัยคุกคามทางไซเบอร์ที่ส่งผลต่อระบบคอมพิวเตอร์ อุปกรณ์ โครงสร้างเครือข่าย หรือระบบงานโดยรวมอย่างรุนแรง หรือมีเหตุอันควรเชื่อได้ว่า ผู้โจมตี มีความมุ่งหมายที่จะทำให้ระบบและข้อมูลของหน่วยงานเสียหายจนไม่สามารถทำงานหรือให้บริการได้	- ซอฟต์แวร์เรียกค่าไถ่ (Ransomware) - Sniffing - Social Engineering - Password Attack - Insider Treats - SQL Injection - Form Jacking

'ระดับความรุนแรง ...

ระดับความรุนแรงของภัยคุกคามทางไซเบอร์ (Security Level)	คำอธิบาย	ประเภท/รูปแบบของภัยคุกคาม
๓ ระดับร้ายแรง (Extreme)	ภัยคุกคามทางไซเบอร์ที่ส่งผลต่อระบบ คอมพิวเตอร์ อุปกรณ์ โครงสร้าง เครือข่าย หรือระบบงาน อย่างรุนแรง หรือมีเหตุอันควรเชื่อได้ว่า ผู้โจมตีจะทำให้ระบบและข้อมูลของหน่วยงานเสียหาย จนไม่สามารถทำงานหรือให้บริการได้ ส่งผลเสียหายเป็นวงกว้างซึ่งอาจทำให้หน่วยงานอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่ออาชญกรรมตามประมวลกฎหมายอาญา	- ผู้บุกรุก (Hacker)

➢ **ผลกระทบต่อการทำงานของระบบ (functional impact)**

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
ไม่มีผลกระทบ (None)	ไม่มีผลกระทบต่อการดำเนินงาน
ระดับต่ำ (Low)	ส่งผลให้การปฏิบัติงานตามภารกิจหลักมีความล่าช้า แต่ยังสามารถดำเนินงานต่อไปได้
ระดับกลาง (Medium)	ส่งผลให้งานตามภารกิจหลักไม่สามารถดำเนินการได้บางส่วน
ระดับสูง (High)	ส่งผลให้งานตามภารกิจหลักหยุดชะงัก

➢ **ผลกระทบต่อข้อมูล (information impact)**

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
ไม่มีข้อมูลรั่วไหล (None)	ไม่มีข้อมูลรั่วไหล ถูกเปลี่ยนแปลง ทำลาย หรือเข้าถึง โดยที่ไม่ได้รับอนุญาต
ละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach)	มีการละเมิดความลับของข้อมูลส่วนบุคคลซึ่งมีการเข้าถึง หรือเปิดเผยข้อมูลส่วนบุคคล
ละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach)	มีการละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคลซึ่งมีการเปลี่ยนแปลงแก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน
ละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach)	มีการละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคลซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

/ระดับ ...

➢ **ระดับความสามารถในการกู้คืน (recoverability effort)**

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
Regular	เวลาในการกู้คืนสามารถคาดการณ์ได้ โดยใช้ทรัพยากรที่มี
Supplemented	เวลาในการกู้คืนสามารถคาดการณ์ได้ แต่ต้องมีการจัดหาทรัพยากรเพิ่ม
Extended	เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือจากภายนอก
Not Recoverable	การกู้คืนไม่สามารถทำได้ ใช้กับสถารการณ์ที่ข้อมูลได้รั่วไหลสู่สาธารณะแล้ว เป็นต้น ให้ใช้วิธีการติดตามและจำกัดการแพร่กระจายรวมถึงการเยียวยาผลกระทบ

แม้ว่าหน่วยงานจะจัดให้มีมาตรการต่าง ๆ เพื่อป้องกันหรือควบคุมมิให้เกิดภัยคุกคามทางไซเบอร์ขึ้นแล้ว ก็ตาม แต่หน่วยงานก็ยังคงต้องเตรียมความพร้อมอยู่เสมอเพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจหลีกเลี่ยงได้ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) จึงเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

๓.๑ การกำหนดวิธีการที่จะใช้ในการตรวจจับ Incident ซึ่งขึ้นอยู่กับระบบงานที่ใช้อยู่ รูปแบบของความพยายามโจมตี และกลไกในการปกป้องระบบ เพราะระบบการป้องกันจะแจ้งเตือน (Alert) หรือเก็บบันทึกข้อมูล (Log) เพื่อใช้ในการวิเคราะห์หาความผิดปกติ และมีการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบ

อุปกรณ์ที่ใช้เพื่อการป้องกันและตรวจจับต้องพิจารณาตามความเหมาะสมกับระบบที่ต้องการป้องกัน และต้องทำการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้น ๆ ซึ่งข้อมูลการแจ้งเตือนเพื่อตรวจจับการบุกรุกระบบคอมพิวเตอร์และเครือข่ายมีดังนี้

๓.๑.๑ <u>ประเภท Alert</u>

(๑) IPS ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีในระบบเครือข่าย มีการแจ้งเตือน เมื่อพบสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก

(๒) SIEM ระบบตรวจจับความผิดปกติโดยใช้ข้อมูล Log จากระบบอื่น ๆ เพื่อนำมาวิเคราะห์ โดยต้องตั้งค่า Rule set โดยผู้เชี่ยวชาญ และเหมาะสมกับสภาพแวดล้อมที่เชื่อมต่ออยู่กับ SIEM สามารถทำงานร่วมกับ EDR โดยตรวจจับภัยคุกคามจากการวิเคราะห์ EDR สามารถระบุภัยคุกคามที่อาจเกิดขึ้น เช่น มัลแวร์ แรนซัมแวร์ ความพยายามฟิชชิ่ง และช่องโหว่แบบ zero-day (ช่องโหว่ที่ไม่รู้จักก่อนหน้านี้)

(๓) Anti-Malware ทำหน้าที่ตรวจจับโปรแกรมประสงค์ร้าย ทำงานทั้งในระดับเครือข่ายและ Host การตรวจเจอ Malware ในระบบเป็นข้อบ่งชี้ได้ทั้งที่กำลังพยายามโจมตีและการโจมตีได้สำเร็จแล้ว

/(๔) Third-Party ...

(๔) Third-Party บริการสอดส่องดูแลความผิดปกติที่เกิดขึ้นกับระบบ หรือระบบของหน่วยงานถูกนำไปโจมตีระบบอื่น ๆ ภายนอกองค์กรซึ่งบ่งบอกได้ว่าระบบภายในหน่วยงานได้ถูกยึดครองโดยผู้ไม่ประสงค์ดี และนำไปใช้สร้างความเสียหาย

๓.๑.๒ ประเภท Log

(๑) Operating System and Application Log ข้อมูลจาก Log ของ OS และ Application ที่ประกอบไปด้วยการบันทึกเหตุการณ์หลายประเภท สามารถถูกใช้ในการตรวจจับภัยคุกคามบางอย่างได้ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์

(๒) Network Device Log อุปกรณ์เครือข่ายที่มีการบันทึกข้อมูลที่ผ่านเข้าออกเครือข่าย สามารถถูกใช้ในการตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์

๓.๑.๓ ข้อมูลจากแหล่งสาธารณะข้อมูลช่องโหว่และวิธีการโจมตีระบบรูปแบบใหม่สามารถถูกใช้เป็นข้อบ่งชี้ภัยคุกคามได้

๓.๑.๔ บุคคลที่ทำหน้าที่แจ้งเตือนบุคคลภายในองค์กร บุคลากรทุกตำแหน่งสามารถเข้ารับการฝึกฝน เพื่อช่วยสอดส่องดูแล

๓.๒ การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติเมื่อได้รับแจ้ง

การวิเคราะห์ภัยคุกคามเพื่อให้การดำเนินการต่อไปสามารถทำได้เร็วและถูกต้อง ใช้การวิเคราะห์ความผิดปกติเมื่อได้รับแจ้งดังนี้

๓.๒.๑ log Retention Policy คือ การใช้ Log จากอุปกรณ์ต่าง ๆ เช่น IPS, Network Devices เป็นต้น จะมีความสำคัญเป็นอย่างมากในการวิเคราะห์หาสาเหตุการโจมตี และบันทึกเหตุการณ์เก็บไว้เพื่อหลักฐานทางกฎหมายหรือเรียกดูในอนาคต จึงต้องมีการเก็บรักษาไว้เป็นอย่างดี และตามระยะเวลาตามกฎหมายกำหนด

๓.๒.๒ Clock Synchronization อุปกรณ์ ทุกชิ้นบนเครือข่ายต้องได้รับการ Synchronize เวลาให้ตรงกันอยู่เสมอเพื่อทำให้การ Correlate Event ทำได้ง่าย

๓.๒.๓ Sniff and Analyze Network Data ทำการดักจับข้อมูลทางเครือข่ายเพื่อนำมาวิเคราะห์ข้อมูล

๓.๒.๔ Seek Assistance เมื่อทีมตอบสนองไม่สามารถดำเนินการวิเคราะห์ incident เพื่อหาสาเหตุที่แท้จริงได้เพื่อกำจัดผู้บุกรุกออกจากระบบ จะใช้บริการให้คำแนะนำปรึกษาจากภายนอก เช่น CERT ต่าง ๆ

(๔) ดำเนินการจัดให้มีบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (รายละเอียดปรากฏตามภาคผนวก ๓)

/(๕) จัดทำบันทึก ...

(๕) จัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) โดยบันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ ทุกขั้นตอนตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย พร้อมเวลาที่เกิดเหตุและระยะเวลาที่ใช้ ลงวันที่และลงนามโดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้น ๆ (รายละเอียดปรากฏตามภาคผนวก ๔)

(๖) กรณีจะต้องจัดให้มีการรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ผู้ที่เกี่ยวข้องทราบ ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ (ประกาศฯ) ดังนี้

(ก) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นตาม ข้อ ๔ แห่งประกาศฯ ให้ใช้แบบฟอร์ม ก๑ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๕)

(ข) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบตาม ข้อ ๕ แห่งประกาศฯ ให้ใช้แบบฟอร์ม ก๒ รายงานไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ภายในระยะเวลา ๒๔ ชั่วโมง โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๕)

(ค) จัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของสำนักงานเศรษฐกิจการคลัง <u>ภายในวันที่ ๓๑ มกราคม ของปีถัดไป</u> ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสาร ก๓ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๕)

นอกจากนี้ สำนักงานเศรษฐกิจการคลังได้ดำเนินการตามแนวปฏิบัติพื้นฐาน (Security Control Baselines) การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (รายละเอียดปรากฏตามภาคผนวก ๖)

๑๐.๓ <u>ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)</u>

การดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ โดยควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป โดยดำเนินการดังต่อไปนี้

/(๑) จำกัดขอบเขต ...

(๑) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๒) เรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(๓) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(๔) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(๕) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ให้บริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

นอกจากนี้ สำนักงานเศรษฐกิจการคลังดำเนินการตามแนวปฏิบัติพื้นฐาน (Security Control Baselines) เพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery) ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (รายละเอียดปรากฏตามภาคผนวก ๗)

๑๐.๔ <u>ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์</u> (Post-Incident activity)

การกำหนดขั้นตอน วิธี ปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้สามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไข จุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้จะต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็นเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวล กฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) ทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

นอกจากนี้ สำนักงานเศรษฐกิจการคลังดำเนินการตามแนวปฏิบัติพื้นฐาน (Security Control Baselines) ของกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity) ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (รายละเอียดปรากฏตามภาคผนวก ๘)

/๑๐.๕ <u>การจัดทำ</u> ...

๑๐.๕ <u>การจัดทำรายการตรวจสอบการจัดการเหตุการณ์</u> (Incident Handling Checklist)

ต้องจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ซึ่งเป็นแนวทางเกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการ โดยสามารถใช้ข้อมูลเพื่อประกอบการพิจารณาความเหมาะสมในการจัดทำรายการตรวจสอบของตนเองได้ (รายละเอียดปรากฏตามภาคผนวก ๙)

แหล่งที่มา

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖

- NIST SP ๘๐๐-๖๑r๒ Computer Security Incident Handling Guide

- ACSC Cyber Incident Response Plan Guidance
