THE NATIONAL CYBER INCIDENT RESPONSE PLAN OF THAILAND (Draft)

(ร่าง) แผนรับมือเหตุการณ์ทางไซเบอร์

สำหรับการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประจำปีงบประมาณ พ.ศ.๒๕๖๕
(Thailand's National Cyber Exercise 2022)

NCSA สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

(ร่าง) แผนรับมือเหตุการณ์ทางไซเบอร์

The National Cyber Incident Response Plan of Thailand (Draft)

สำหรับการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงาน
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประจำปีงบประมาณ พ.ศ.๒๕๖๕
(Thailand's National Cyber Exercise 2022)
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

(ร่าง) แผนรับมือเหตุการณ์ทางไซเบอร์

The National Cyber Incident Response Plan of Thailand (Draft)

พิมพ์ครั้งที่ ๑ มกราคม ๒๕๖๕

จำนวนพิมพ์ ๓๐๐ เล่ม

เจ้าของ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

พิมพ์ที่

บริษัท ทริปเพิ้ล กรุ๊ป จำกัด www.triple-group.co.th

สารบัญ

สารบัญ (ต่อ)

บทที่ ๑
บทนำ

บทที่ ๑
บทนำ

หลักการและเหตุผล

(ร่าง) แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕ – ๒๕๗๐ ซึ่งอยู่ระหว่างเสนอคณะรัฐมนตรีเพื่อให้ความเห็นชอบ เป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติ และในสถานการณ์ที่อาจจะเกิด หรือเกิดภัยคุกคามทางไซเบอร์ ได้กำหนดแนวทางการดำเนินงานเพื่อขับเคลื่อนประเด็นยุทธศาสตร์ที่ ๑ สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน กลยุทธ์ที่ ๑.๑ เพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยจะต้องมีแผนรองรับสถานการณ์ฉุกเฉินด้านไซเบอร์ เพื่อใช้ในการรับมือและฟื้นฟูบริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประกอบกับมาตรา ๒๒ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มีหน้าที่และอำนาจที่สำคัญในการดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ รวมทั้งการยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

สกมช. จึงได้จัดทำ (ร่าง) แผนรับมือเหตุการณ์ทางไซเบอร์ (DRAFT Thailand's National Cyber Incident Response Plan) ฉบับนี้ขึ้น เพื่อเป็นเอกสารหลักสำหรับผู้รับการฝึก เพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ได้แก่ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่นๆ ที่เกี่ยวข้อง ซึ่งจะทำให้มีความรู้ความเข้าใจเพิ่มมากขึ้นเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมทั้งเพื่อทดสอบความถูกต้องเหมาะสมของ (ร่าง) แผนรับมือเหตุการณ์ทางไซเบอร์ ในห้วงการฝึกดังกล่าวก่อนที่จะนำไปพัฒนาเป็นแผนรับมือฉบับจริงต่อไป

วัตถุประสงค์

๑. เพื่อใช้เป็นแผนในการรับมือและฟื้นฟูบริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ได้อย่างเป็นระบบ มีเอกภาพ มีประสิทธิภาพ และทันต่อเหตุการณ์

๒. เพื่อให้เกิดความร่วมมือระหว่าง หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่นๆ ที่เกี่ยวข้องกับการบริหารสถานการณ์วิกฤติระดับชาติ ในการรับมือกับภัยคุกคามทางไซเบอร์

ขอบเขต

ใช้สำหรับหน่วยงานที่เกี่ยวข้องตามที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

บทที่ ๒
แผนสำคัญที่เกี่ยวข้อง

บทที่ ๒
แผนสำคัญที่เกี่ยวข้อง

ยุทธศาสตร์ชาติ ๒๐ ปี (พ.ศ. ๒๕๖๑ - ๒๕๘๐)

ยุทธศาสตร์ชาติ ๒๐ ปี (พ.ศ. ๒๕๖๑ - ๒๕๘๐) ด้านความมั่นคง กำหนดเป้าหมายและประเด็นยุทธศาสตร์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

เป้าหมายที่ ๓ กองทัพ หน่วยงานด้านความมั่นคง ภาครัฐ ภาคเอกชน และภาคประชาชน มีความพร้อมในการป้องกันและแก้ไขปัญหาความมั่นคง

เป้าหมายที่ ๔ ประเทศไทยมีบทบาทด้านความมั่นคงเป็นที่ชื่นชมและได้รับการยอมรับโดยประชาคมระหว่างประเทศ

เป้าหมายที่ ๕ การบริหารจัดการความมั่นคงมีผลสำเร็จที่เป็นรูปธรรมอย่างมีประสิทธิภาพ

ประเด็นยุทธศาสตร์

ข้อ ๔.๒ การป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง

ข้อ ๔.๒.๑ การแก้ไขปัญหาความมั่นคงในปัจจุบัน

ข้อ ๔.๒.๒ การติดตาม เฝ้าระวัง ป้องกัน และแก้ไขปัญหาที่อาจอุบัติขึ้นใหม่

แผนระดับที่ ๒

๑. แผนแม่บทภายใต้ยุทธศาสตร์ชาติ

ประเด็นยุทธศาสตร์ด้านความมั่นคง

ข้อ ๓.๒ แผนย่อยการป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง

๒. แผนปฏิรูปประเทศด้านสื่อสารมวลชน เทคโนโลยีสารสนเทศ

ประเด็นยุทธศาสตร์แผนปฏิรูปประเทศด้านสื่อสารมวลชน เทคโนโลยีสารสนเทศ

ข้อ ๕.๕ การปฏิรูปการบริหารจัดการความปลอดภัยไซเบอร์ / กิจการอวกาศและระบบและเครื่องมือด้านการสื่อสารมวลชนและโทรคมนาคมเพื่อสนับสนุนภารกิจการป้องกันบรรเทาสาธารณภัย ภายใต้กิจกรรมที่ ๑ การปกป้องคุ้มครองและรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญด้านสารสนเทศของประเทศ

๓. แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒

ยุทธศาสตร์ที่ ๕ การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน

แนวทางการพัฒนาที่ ๓.๒ การพัฒนาเสริมสร้างศักยภาพการป้องกันประเทศเพื่อเตรียมความพร้อมในการรับมือภัยคุกคาม ทั้งการทหารและภัยคุกคามอื่นๆ

ยุทธศาสตร์ที่ ๗ การพัฒนาโครงสร้างพื้นฐานและระบบโลจิสติกส์

แนวทางการพัฒนาที่ ๓.๕ การพัฒนาเศรษฐกิจดิจิทัล

๔. นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. ๒๕๖๒ – ๒๕๖๕)

นโยบายที่ ๑๐ เสริมสร้างความมั่นคงปลอดภัยไซเบอร์ รองรับวัตถุประสงค์ ๓.๔.๕ เพื่อพัฒนาศักยภาพของภาครัฐ และส่งเสริมบทบาทและความเข้มแข็งของทุกภาคส่วนในการรับมือกับภัยคุกคามทุกรูปแบบที่กระทบกับความมั่นคง

แผนที่ ๑๕ การป้องกันและแก้ไขความมั่นคงทางไซเบอร์

แผนระดับที่ ๓

๑. นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ ๒๕๖๑ – ๒๕๘๐)

ยุทธศาสตร์ที่ ๖ สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

แผนงาน ข้อ ๓ สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัลและการทำธุรกรรมออนไลน์

๒. แผนปฏิบัติการด้านดิจิทัลเพื่อเศรษฐกิจและสังคมระยะ ๕ ปี (พ.ศ. ๒๕๖๑-๒๕๖๕)

เป้าหมายที่ ๕ สร้างความเชื่อมั่น

ประเด็นขับเคลื่อน ๕.๑ การเสริมสร้างความมั่นคงปลอดภัยไซเบอร์

ประเด็นขับเคลื่อน ๕.๒ ขับเคลื่อนการพัฒนากฎหมายและมาตรฐานดิจิทัล

เป้าหมายที่ ๖ พัฒนากำลังคนดิจิทัล

ประเด็นขับเคลื่อน ๖.๑ การพัฒนากำลังคนและประชาชนสู่ยุคดิจิทัล

๓. ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ ๒๕๖๐-๒๕๖๕)

ประเด็นยุทธศาสตร์ที่ ๑ เสริมสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วนในการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ

ประเด็นยุทธศาสตร์ที่ ๒ ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์

ประเด็นยุทธศาสตร์ที่ ๓ ปกป้องผลประโยชน์และความมั่นคงของชาติให้รอดพ้นจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่

ประเด็นยุทธศาสตร์ที่ ๔ เสริมสร้างระบบเศรษฐกิจดิจิทัล

ประเด็นยุทธศาสตร์ที่ ๕ สร้างความตระหนักและส่งเสริมความร่วมมือภายในประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประเด็นยุทธศาสตร์ที่ ๖ เพื่อส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซในทางที่เหมาะสม

ประเด็นยุทธศาสตร์ที่ ๗ ส่งเสริมงานด้านการป้องกันและปราบปรามอาชญากรรม

ประเด็นยุทธศาสตร์ที่ ๘ ส่งเสริมบทบาทที่สร้างสรรค์ของไทยในความร่วมมือเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาคและระดับนานาชาติ

๔. แผนเตรียมพร้อมแห่งชาติ (พ.ศ. ๒๕๖๐-๒๕๖๕)

ยุทธศาสตร์ที่ ๓ การเสริมสร้างความร่วมมือ การเตรียมพร้อมรับมือภัยคุกคามกับต่างประเทศ

กลยุทธ์ ข้อ ๔ เสริมสร้างความสัมพันธ์และความร่วมมือการเตรียมพร้อมด้านวิกฤตการณ์ความมั่นคงกับต่างประเทศ อาทิ การก่อวินาศกรรม การก่อการร้าย ภัยความมั่นคงทางไซเบอร์ ภัยความมั่นคงทางอวกาศ โรคติดต่ออุบัติใหม่ ให้สอดคล้องกับนโยบายรัฐบาล นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติและยุทธศาสตร์ความมั่นคงเฉพาะด้านที่เกี่ยวข้อง

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มีการกำหนดเนื้อหาในส่วนที่เกี่ยวข้องกับการรับมือกับภัยคุกคามทางไซเบอร์ไว้ในหมวดที่ ๓ การรักษาความมั่นคงปลอดภัยไซเบอร์ ส่วนที่ ๔ การรับมือกับภัยคุกคามทางไซเบอร์ มาตราที่ ๕๘ – ๖๙

บทที่ ๓
หน้าที่และความรับผิดชอบ

บทที่ ๓
หน้าที่และความผิดชอบ

๑. คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

๑.๑ เสนอนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมและสนับสนุนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๔๒ และมาตรา ๔๓ ต่อคณะรัฐมนตรีเพื่อให้ความเห็นชอบ ซึ่งต้องเป็นไปตามแนวทางที่กำหนดไว้ในมาตรา ๔๒

๑.๒ กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๑.๓ จัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เสนอต่อคณะรัฐมนตรี สำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบาย ยุทธศาสตร์และแผนระดับชาติและกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

๑.๔ กำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน

๑.๕ กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ เจ้าหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๖ กำหนดกรอบการประสานความร่วมมือกับหน่วยงานอื่นทั้งในประเทศและต่างประเทศที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๗ แต่งตั้งและถอดถอนเลขาธิการ

๑.๘ มอบหมายการควบคุมและกำกับดูแล รวมถึงการออกข้อกำหนด วัตถุประสงค์ หน้าที่และอำนาจ และกรอบการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานของรัฐ หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๑. ๙ ติดตามและประเมินผลการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่บัญญัติไว้ในพระราชบัญญัตินี้

๑.๑๐ เสนอแนะและให้ความเห็นต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ หรือคณะรัฐมนตรี เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๑๑ เสนอแนะต่อคณะรัฐมนตรีในการจัดให้มีหรือปรับปรุงกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๑๒ จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญหรือแนวทางการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้คณะรัฐมนตรีทราบ

๑.๑๓ ปฏิบัติการอื่นใดตามที่บัญญัติไว้ในพระราชบัญญัตินี้ หรือคณะรัฐมนตรีมอบหมาย

๒. คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)

๒.๑ ติดตามการดำเนินการตามนโยบายและแผนตามมาตรา ๙ (๑) และมาตรา ๔๒

๒.๒ ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ตามมาตรา ๖๑ มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ มาตรา ๖๕ และมาตรา ๖๖

๒.๓ กำกับดูแลการดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ และการเผชิญเหตุและนิติวิทยาศาสตร์ทางคอมพิวเตอร์

๒.๔ กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

๒.๕ กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล โดยอย่างน้อยต้องกำหนดหน้าที่ให้หน่วยงานควบคุมหรือกำกับดูแลต้องกำหนดมาตรฐานที่เหมาะสมเพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานของรัฐ

๒.๖ กำหนดระดับของภัยคุกคามทางไซเบอร์ พร้อมทั้งรายละเอียดของมาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ในแต่ละระดับเสนอต่อคณะกรรมการ

๒.๗ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ เพื่อเสนอต่อคณะกรรมการพิจารณาสั่งการ เมื่อมีหรือคาดว่าจะมีภัยคุกคามทางไซเบอร์ในระดับร้ายแรงขึ้น

๓. คณะอนุกรรมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง (อรร.)

เป็นคณะกรรมการที่จะมีการจัดตั้งขึ้นตาม (ร่าง) ระเบียบคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยการมอบอำนาจ และการกำหนดให้หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ถูกคุกคามเข้าร่วมดำเนินการ ประสานงาน และให้การสนับสนุน ในการปฏิบัติการเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์ พ.ศ. .... โดยอาศัยอำนาจตามความในมาตรา ๑๔ วรรคสอง แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยมีหน้าที่และอำนาจ รายละเอียดตามผนวก ข สรุปได้ดังต่อไปนี้

๓.๑ ร่วมกันปฏิบัติการเพื่อรับมือกับภัยคุกคามทางไซเบอร์

๓.๒ ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ตามมาตรา ๖๑ มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ มาตรา ๖๕ และมาตรา ๖๖ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๒

๓.๓ ปฏิบัติการอื่นใดตามที่ กกม. มอบหมาย

๔. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

๔.๑ เสนอแนะและสนับสนุนในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๙ ต่อคณะกรรมการ

๔.๒ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง (๔) เสนอต่อ กกม. เพื่อให้ความเห็นชอบ

๔.๓ ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๕๓ และมาตรา ๕๔

๔.๔ ประสานงานและให้ความร่วมมือในการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในประเทศและต่างประเทศในส่วนที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และกำหนดมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์

๔.๕ ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ตามที่ได้รับมอบหมายจากคณะกรรมการ

๔.๖ เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

๔.๗ ปฏิบัติการ ประสานงาน สนับสนุน และให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์หรือตามคำสั่งของคณะกรรมการ

๔.๘ ดำเนินการและให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๔.๙ เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้างความตระหนักด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกันเพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน

๔.๑๐ เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน

๔.๑๑ เป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชน ทั้งในประเทศและต่างประเทศ

๕. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT)

มีหน้าที่และอำนาจ รายละเอียดตามประกาศ กมช. เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ สรุปได้ดังต่อไปนี้

๕.๑ การดำเนินมาตรการเชิงรุกเพื่อป้องกันและเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์

๕.๒ การดำเนินมาตรการเชิงรับเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

๕.๓ การดำเนินมาตรการด้านการบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

๖. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectorial CERT)

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยมีหน้าที่และความรับผิดชอบในด้านการประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตลอดจนมีหน้าที่ในการช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับสำนักงาน หน่วยงานควบคุมหรือกำกับดูแล พนักงานเจ้าหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยภารกิจหรือให้บริการ รายละเอียดตามประกาศ กมช. เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ สรุปได้ดังต่อไปนี้

๖.๑ ภารกิจหรือให้บริการในด้านการประสานงาน

๖.๒ ภารกิจหรือให้บริการในด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์

๖.๓ ภารกิจหรือให้บริการในด้านการรับมือและแก้ไขภัยคุกคามทางไซเบอร์

๖.๔ ภารกิจหรือให้บริการในด้านการดำเนินมาตรการด้านการบริหารจัดการคุณภาพ

๗. หน่วยงานควบคุมหรือกำกับดูแล

๗.๑ กำหนดมาตรฐานที่เหมาะสมเพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานของรัฐ

๗.๒ เข้าร่วมดำเนินการ ประสานงาน และให้การสนับสนุน กกม. ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ตามมาตรา ๖๑ มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ มาตรา ๖๕ และมาตรา ๖๖

๗.๓ ดำเนินการให้เป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๗.๔ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

๗.๕ ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง (๔) ด้วย

๗.๖ แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงาน

๗.๗ ตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมกำกับหรือดูแลของตน หากพบว่าหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่ได้มาตรฐาน ให้หน่วยงานควบคุมหรือกำกับดูแลนั้นรีบแจ้งให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ต่ำกว่ามาตรฐานแก้ไขให้ได้มาตรฐานโดยเร็ว หากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นยังคงเพิกเฉยไม่ดำเนินการ หรือไม่ดำเนินการให้แล้วเสร็จภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด ให้หน่วยงานควบคุมหรือกำกับดูแลส่งเรื่องให้ กกม. พิจารณาโดยไม่ชักช้า

๗.๘ เมื่อปรากฏแก่หน่วยงานควบคุมหรือกำกับดูแล หรือเมื่อหน่วยงานควบคุมหรือกำกับดูแลได้รับแจ้งเหตุตามมาตรา ๕๘ ให้หน่วยงานควบคุมหรือกำกับดูแล ร่วมกับหน่วยงานตามมาตรา ๕๐

รวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ และดำเนินการ ดังต่อไปนี้

(๑) สนับสนุนและให้ความช่วยเหลือแก่หน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน และให้ความร่วมมือและประสานงานกับสำนักงาน ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

(๒) แจ้งเตือนหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน รวมทั้งหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอื่นที่เกี่ยวข้องโดยเร็ว

๘. หน่วยงานของรัฐ

๘.๑ ดำเนินการให้เป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๘.๒ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

๘.๓ ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง (๔) ด้วย

๘.๔ แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงาน

๘.๕ ดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว

๙. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๙.๑ เข้าร่วมดำเนินการ ประสานงาน และให้การสนับสนุน กกม. ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ตามมาตรา ๖๑ มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ มาตรา ๖๕ และมาตรา ๖๖

๙.๒ ดำเนินการให้เป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๙.๓ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

๙.๔ ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง (๔) ด้วย

๙.๕ แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงาน

๙.๖ แจ้งรายชื่อและข้อมูลการติดต่อของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ไปยังสำนักงาน หน่วยงานควบคุมหรือกำกับดูแลของตน และหน่วยงานตามมาตรา ๕๐ ภายในสามสิบวันนับแต่วันที่คณะกรรมการประกาศตามมาตรา ๔๙ วรรคสอง และมาตรา ๕๐ วรรคสอง หรือนับแต่วันที่คณะกรรมการมีคำวินิจฉัยตามมาตรา ๕๑ แล้วแต่กรณี โดยอย่างน้อยเจ้าของกรรมสิทธิ์ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ต้องเป็นบุคคลซึ่งรับผิดชอบในการบริหารงานของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น

๙.๗ ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง

ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงานภายในสามสิบวันนับแต่วันที่ดำเนินการแล้วเสร็จ

๙.๘ ต้องกำหนดให้มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน ตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแล และตามประมวลแนวทางปฏิบัติ รวมถึงระบบมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการหรือ กกม. กำหนด และต้องเข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น

๙.๙ เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในส่วนที่ ๔ ทั้งนี้ กกม. อาจกำหนดหลักเกณฑ์และวิธีการการรายงานด้วยก็ได้

๙.๑๐ ดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว

๑๐. สภาความมั่นคงแห่งชาติ

ในกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ให้เป็นหน้าที่และอำนาจของสภาความมั่นคงแห่งชาติ ในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายว่าด้วยสภาความมั่นคงแห่งชาติ และกฎหมายอื่นที่เกี่ยวข้อง โดยมีกฎหมายที่สำคัญ ได้แก่

๑๐.๑ พระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. ๒๕๔๘

๑๐.๒ พระราชบัญญัติสภาความมั่นคงแห่งชาติ พ.ศ. ๒๕๕๙

ทั้งนี้ สภาความมั่นคงแห่งชาติอาจพิจารณาการใช้กฎหมายทั้งสองฉบับข้างต้น ตามความเหมาะสมของสถานการณ์ และจะมีการพิจารณาใช้กลไกปฏิบัติ ประกอบด้วย แผนเตรียมพร้อมแห่งชาติ แผนบริหารวิกฤตการณ์ ร่วมกับแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕ – ๒๕๗๐ รวมถึง แผนรับมือเหตุการณ์ทางไซเบอร์ฉบับนี้ และกฎหมายอื่นๆ ที่เกี่ยวข้อง ต่อไป

บทที่ ๔
แนวทางปฏิบัติในการรับมือเหตุภัยคุกคามทางไซเบอร์

บทที่ ๔
แนวทางปฏิบัติในการรับมือเหตุภัยคุกคามทางไซเบอร์

กล่าวโดยทั่วไป

ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นต่อ หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จนส่งผลกระทบต่อการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ สามารถจำแนกหมวดหมู่ตามประกาศ กมช. เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รายละเอียดตามผนวก ค สรุปได้ดังนี้

๑. เหตุการณ์จำลอง และ การฝึกจู่โจม ของหน่วยงานเอง (Training and Exercises)
๒. การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
๓. การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
๔. การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
๕. การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
๖. การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
๗. การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
๘. การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
๙. เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
๑๐. เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

ความมุ่งหมาย

๑. เพื่อให้การดำเนินการรับมือและฟื้นฟูบริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ เป็นไปตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดได้อย่างเป็นระบบ มีเอกภาพ มีประสิทธิภาพ และทันต่อเหตุการณ์

๒. เพื่อให้ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่นๆ ที่เกี่ยวข้องกับการบริหารสถานการณ์วิกฤติระดับชาติ มีความเข้าใจขั้นตอนการปฏิบัติต่างๆ และมีความพร้อมในการปฏิบัติงานในหน้าที่ความรับผิดชอบ

การปฏิบัติ

๑. แนวทางปฏิบัติ เพื่อให้ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่นๆ ที่เกี่ยวข้องกับการบริหารสถานการณ์วิกฤติระดับชาติ มีความเข้าใจขั้นตอนการปฏิบัติต่างๆ และมีความพร้อมในการปฏิบัติงานในหน้าที่ความรับผิดชอบ จึงแบ่งขั้นตอนการปฏิบัติออกเป็น ๔ ขั้น ตามประกาศ กมช. เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ สรุปได้ดังนี้

๑.๑ ขั้นตอนที่ ๑: การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์

การดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (Preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ

๑.๒ ขั้นตอนที่ ๒: การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์

แม้ว่าหน่วยงานจะจัดให้มีมาตรการต่าง ๆ เพื่อป้องกันหรือควบคุมมิให้เกิดภัยคุกคามทางไซเบอร์ขึ้นแล้วก็ตาม แต่หน่วยงานก็ยังคงต้องเตรียมความพร้อมอยู่เสมอเพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจหลีกเลี่ยงได้ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) จึงเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

๑.๓ ขั้นตอนที่ ๓: การระงับภัยคุกคามทางไซเบอร์ ปราบปรามภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบงานที่ได้รับผลกระทบ

เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือเมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์หน่วยงานควรกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, Eradication, and Recovery) โดยการดำเนินการดังกล่าว ควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป

๑.๔ ขั้นตอนที่ ๔ : การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-incident Activity) นั้น หน่วยงานควรกำหนดขั้นตอน วิธีปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง (โดยการเก็บข้อมูลบางประเภทนั้นอาจจำเป็นต้องดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไปในระหว่างที่ต้องระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตี)

เมื่อมีการเก็บรวบรวมข้อมูลและหลักฐานที่จำเป็นแล้ว หน่วยงานควรนำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคามทางไซเบอร์ โดยอาจจัดทำเป็นรายสัปดาห์หรือรายเดือน เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน และกำหนดขั้นตอนที่หน่วยงานควรดำเนินการ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ในลักษณะดังกล่าวขึ้นอีกในอนาคต

๒. กลไกการแก้ไขปัญหา

๒.๑ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

๒.๑.๑ ในขั้นตอนที่ ๑ ดำเนินการตามอำนาจหน้าที่ในมาตรา ๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมทั้งอำนวยการ และกำกับดูแลการปฏิบัติตามข้อ ๑.๑

๒.๑.๒ ในขั้นตอนที่ ๒ เมื่อได้รับแจ้ง และ/หรือรายงาน จาก สกมช. ให้ กมช. ยืนยันว่าเหตุการณ์ที่เกิดขึ้นเป็นเหตุจำเป็นเร่งด่วน และเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติหรือไม่

๒.๑.๓ ในขั้นตอนที่ ๓ ในกรณีที่เป็นเหตุจำเป็นเร่งด่วน และเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ

(๑) สั่งการให้ สกมช. แจ้งไปยัง สำนักงาน สมช. เพื่อดำเนินการตามกฎหมายว่าด้วยสภาความมั่นคงแห่งชาติ

(๒) อาจมอบหมายให้เลขาธิการ กมช. มีอำนาจดำเนินการได้ทันทีเท่าที่จำเป็นเพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าได้โดยไม่ต้องยื่นคำร้องต่อศาล แต่หลังจากการดำเนินการดังกล่าว ให้แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็ว

(๓) ติดตามสถานการณ์ ตลอดจนกำกับดูแลการแก้ไขปัญหาจากภัยคุกคามทางไซเบอร์

๒.๑.๔ ในขั้นตอนที่ ๔ รับทราบรายงานผลการแก้ไขปัญหาจากภัยคุกคามทางไซเบอร์ รวมทั้งอำนวยการ และกำกับดูแลการปฏิบัติตามข้อ ๑.๔

๒.๒ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)

๒.๒.๑ ในขั้นตอนที่ ๑ ดำเนินการตามอำนาจหน้าที่ในมาตรา ๑๓ แห่ง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมทั้งอำนวยการ และกำกับดูแลการปฏิบัติตามข้อ ๑.๑

๒.๒.๒ ในขั้นตอนที่ ๒ เมื่อได้รับแจ้ง และ/หรือรายงาน จาก สกมช. หรือเมื่อปรากฏแก่ กกม. ว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงให้ กกม. ยืนยันว่าเหตุการณ์ที่เกิดขึ้นเป็นหรือคาดว่าจะเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรงหรือไม่

๒.๒.๓ ในขั้นตอนที่ ๓ เมื่อปรากฏแก่ กกม. ว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

(๑) ออกคำสั่งให้ สกมช. ดำเนินการ ดังต่อไปนี้

(๑.๑) รวบรวมข้อมูล หรือพยานเอกสาร พยานบุคคล พยานวัตถุที่เกี่ยวข้องเพื่อวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

(๑.๒) สนับสนุน ให้ความช่วยเหลือ และเข้าร่วมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(๑.๓) ดำเนินการป้องกันเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกิดจากภัยคุกคามทางไซเบอร์ เสนอแนะหรือสั่งการให้ใช้ระบบที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการหาแนวทางตอบโต้หรือการแก้ไขปัญหาเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๑.๔) สนับสนุน ให้ สกมช. และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชนให้ความช่วยเหลือและเข้าร่วมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(๑.๕) แจ้งเตือนภัยคุกคามทางไซเบอร์ให้ทราบโดยทั่วกัน ทั้งนี้ ตามความจำเป็นและเหมาะสม โดยคำนึงถึงสถานการณ์ ความร้ายแรงและผลกระทบจากภัยคุกคามทางไซเบอร์นั้น

(๑.๖) ให้ความสะดวกในการประสานงานระหว่างหน่วยงานของรัฐที่เกี่ยวข้องและหน่วยงานเอกชนเพื่อจัดการความเสี่ยงและเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๒) ในกรณีที่มีความจำเป็นเพื่อการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้ กกม. มีคำสั่งให้หน่วยงานของรัฐให้ข้อมูล สนับสนุนบุคลากรในสังกัด หรือใช้เครื่องมือทางอิเล็กทรอนิกส์ที่อยู่ในความครอบครองที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๓) ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และดำเนินมาตรการที่จำเป็น และให้ กกม. มีหนังสือถึงหน่วยงานของรัฐที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กระทำการหรือระงับการดำเนินการใด ๆ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสมและมีประสิทธิภาพตามแนวทางที่ กกม. กำหนด รวมทั้งร่วมกัน

บูรณาการในการดำเนินการเพื่อควบคุม ระงับ หรือบรรเทาผลที่เกิดจากภัยคุกคามทางไซเบอร์นั้นได้อย่างทันท่วงที

(๔) ออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ดำเนินการ ดังต่อไปนี้

(๔.๑) เฝ้าระวังคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใดระยะเวลาหนึ่ง

(๔.๒) ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

(๔.๓) ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์เพื่อจัดการข้อบกพร่องหรือกำจัดชุดคำสั่งไม่พึงประสงค์ หรือระงับบรรเทาภัยคุกคามทางไซเบอร์ที่ดำเนินการอยู่

(๔.๔) รักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์

(๔.๕) เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์

ในกรณีมีเหตุจำเป็นที่ต้องเข้าถึงข้อมูลตามข้อ ๔.๕ ให้ กกม. มอบหมายให้ เลขาธิการ กมช. ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้เจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือผู้ดูแลระบบคอมพิวเตอร์ ดำเนินการตามคำร้อง ทั้งนี้ คำร้องที่ยื่นต่อศาลต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

๒.๒.๔ ในขั้นตอนที่ ๔ รับทราบรายงานผลการแก้ไขปัญหาจากภัยคุกคามทางไซเบอร์รวมทั้งอำนวยการ และกำกับดูแลการปฏิบัติตามข้อ ๑.๔

๒.๓ คณะอนุกรรมการดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง (อรร.)

สนับสนุนการดำเนินการของ กกม. ตามขั้นตอนในข้อ ๒.๒ และดำเนินการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงตามที่กำหนดไว้ใน (ร่าง) ระเบียบคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยการมอบอำนาจ และการกำหนดให้หน่วยงานควบคุมหรือ

กำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ถูกคุกคามเข้าร่วมดำเนินการประสานงาน และให้การสนับสนุน ในการปฏิบัติการเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์ พ.ศ. ....

๒.๔ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

๒.๔.๑ ในขั้นตอนที่ ๑ ดำเนินการตามอำนาจหน้าที่ในมาตรา ๒๒ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมทั้งดำเนินการ และประสานงาน การปฏิบัติตามข้อ ๑.๑

๒.๔.๒ ในขั้นตอนที่ ๒ เมื่อได้รับแจ้งจากหน่วยงานของรัฐ หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และ/หรือรายงานจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ สกมช. รวบรวมข้อมูลและตรวจสอบว่าเหตุการณ์ที่เกิดขึ้นเป็นหรือคาดว่าจะเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และ/หรือระดับวิกฤติ หรือไม่ พร้อมทั้งดำเนินการแจ้ง และ/หรือรายงานผลการตรวจสอบให้ กกม. และ/หรือ กมช. พิจารณายืนยันระดับของภัยคุกคามทางไซเบอร์ต่อไป

๒.๔.๓ ในขั้นตอนที่ ๓ ภายหลังการรวบรวมข้อมูลและตรวจสอบระดับของภัยคุกคามทางไซเบอร์

(๑) เข้าร่วมดำเนินการกับหน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานตามมาตรา ๕๐ เพื่อรวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์

(๒) ดำเนินการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ตามที่ กกม. มีคำสั่งให้ดำเนินการ (ม.๖๑) ดังนี้

(๒.๑) รวบรวมข้อมูล หรือพยานเอกสาร พยานบุคคล พยานวัตถุที่เกี่ยวข้องเพื่อวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

(๒.๒) สนับสนุน ให้ความช่วยเหลือ และเข้าร่วมในการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(๒.๓) ดำเนินการป้องกันเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกิดจากภัยคุกคามทางไซเบอร์ เสนอแนะหรือสั่งการให้ใช้ระบบที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการหาแนวทางตอบโต้หรือการแก้ไขปัญหาเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๒.๔) สนับสนุน ให้สำนักงาน และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน ให้ความช่วยเหลือและเข้าร่วมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(๒.๕) แจ้งเตือนภัยคุกคามทางไซเบอร์ให้ทราบโดยทั่วกัน ทั้งนี้ตามความจำเป็นและเหมาะสม โดยคำนึงถึงสถานการณ์ ความร้ายแรงและผลกระทบจากภัยคุกคามทางไซเบอร์นั้น

๒.๖ ให้ความสะดวกในการประสานงานระหว่างหน่วยงานของรัฐที่เกี่ยวข้องและหน่วยงานเอกชนเพื่อจัดการความเสี่ยงและเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๒.๔.๔ ในขั้นตอนที่ ๔ ให้เลขาธิการรายงานการดำเนินการตามมาตรา ๖๔ ต่อ กกม. อย่างต่อเนื่อง และเมื่อภัยคุกคามทางไซเบอร์ดังกล่าวสิ้นสุดลง ให้รายงานผลการดำเนินการต่อ กกม. โดยเร็ว

๒.๕ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT)

สนับสนุนการดำเนินการของ สกมช. ตามขั้นตอนในข้อ ๒.๔ และดำเนินการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดไว้ใน ประกาศ กมช. เรื่อง การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. ๒๕๖๔

๒.๖ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectorial CERT)

ดำเนินการตามที่กำหนดไว้ในมาตรา ๕๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และประกาศ กมช. เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. ๒๕๖๔

๒.๖.๑ ในขั้นตอนที่ ๑ สนับสนุนการปฏิบัติตามข้อ ๑.๑ ดังนี้

(๑) ประสานความร่วมมือกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติในการปฏิบัติหน้าที่ด้านการเฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๒) ให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติในการดำเนินภารกิจหรือให้บริการ ซึ่งรวมถึงแต่ไม่จำกัดเฉพาะการดำเนินมาตรการเชิงรุกเพื่อป้องกันและเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ การดำเนินมาตรการเชิงรับเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น และการดำเนินมาตรการด้านการบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นต้น

(๓) ควรให้ความสำคัญกับการแบ่งปันข้อมูลที่เกี่ยวข้องเพื่อประโยชน์ในการเฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์

(๔) อาจร่วมมือกับหน่วยงานอื่น ๆ ที่ดำเนินภารกิจหรือให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ให้แก่หน่วยงานที่มีภารกิจหรือให้บริการในลักษณะเดียวกันหรือมีความเกี่ยวข้องกันกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อช่วยยกระดับความ

สามารถในการดำเนินภารกิจหรือให้บริการด้านต่าง ๆ ของศูนย์ประสานการรักษาความมั่นคงปลอดภัย ตลอดจนการปฏิบัติหน้าที่ในการเฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์

(๕) ดำเนินมาตรการด้านการบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่อยู่ภายใต้การดูแล

๒.๖.๒ ในขั้นตอนที่ ๒ สนับสนุนการปฏิบัติตามข้อ ๑.๒ ดังนี้

(๑) เฝ้าระวังความเสี่ยงและติดตามแนวโน้มของการเกิดภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ รวมถึงดำเนินการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น หรือให้คำเตือนเกี่ยวกับช่องโหว่ที่อาจถูกใช้เป็นช่องทางในการก่อภัยคุกคามทางไซเบอร์ เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดำเนินการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบงานที่มีความสำคัญอื่น ๆ ได้อย่างทันท่วงที

(๒) วิเคราะห์และตรวจสอบข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น รวมถึงการเผยแพร่ข้อมูลที่มีความจำเป็นเพื่อให้หน่วยงาน CII สามารถดำเนินมาตรการป้องกันหรือจัดการกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น เช่น การให้คำแนะนำแก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการตรวจจับเหตุการณ์ที่อาจนำมาสู่การบุกรุก และการวิเคราะห์ข้อมูล เป็นต้น

(๓) ดำเนินการเพื่อให้มีการรับลงทะเบียนข้อมูลและจัดทำบัญชีช่องทางการติดต่อ (point of contact) ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อใช้เป็นช่องทางหลักในการติดต่อสื่อสารระหว่างศูนย์ประสานการรักษาความมั่นคงปลอดภัยกับหน่วยงานดังกล่าว และจัดทำรายชื่อของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบงานที่มีความสำคัญอื่น ๆ ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใช้ในการดำเนินภารกิจหรือให้บริการในกิจการของตน ซึ่งจำเป็นต้องมีการเฝ้าระวัง หรือดำเนินการป้องกันทางไซเบอร์ และปรับปรุงข้อมูลดังกล่าว ให้เป็นปัจจุบันอยู่เสมอ

๒.๖.๓ ในขั้นตอนที่ ๓ สนับสนุนการปฏิบัติตามข้อ ๑.๓ ดังนี้

(๑) เป็นศูนย์กลางในการรับและแจ้งเหตุเกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ ตลอดจนให้การสนับสนุนข้อมูลต่าง ๆ ที่จำเป็นต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อดำเนินการแก้ไขเหตุภัยคุกคามทางไซเบอร์ โดยจัดให้มีช่องทางในการรับและแจ้งเหตุผ่านระบบอิเล็กทรอนิกส์ที่กำหนดขึ้นโดยเฉพาะหรือช่องทางอื่นใดตามที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยกำหนด

(๒) ให้การช่วยเหลือ แนะนำ หรือสนับสนุนหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น และปฏิบัติงานร่วมกับหน่วยงานควบคุมหรือกำกับดูแลในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ดังกล่าว

(๓) เมื่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติแจ้งการเปลี่ยนแปลงระดับ หรือยกระดับการแจ้งเตือน หรือเมื่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยพบการเปลี่ยนแปลงลักษณะของภัยคุกคามทางไซเบอร์หรือผลกระทบต่อภารกิจ หรือการให้บริการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยแจ้งการเปลี่ยนแปลง หรือดำเนินการแจ้งเตือนไปยังหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อให้หน่วยงานดังกล่าวเตรียมความพร้อมในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์

(๔) ให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับสำนักงาน หน่วยงานควบคุมหรือกำกับดูแล พนักงานเจ้าหน้าที่ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒.๖.๔ ในขั้นตอนที่ ๔ สนับสนุนการปฏิบัติตามข้อ ๑.๔ เพื่อได้รับการประสานจากสำนักงาน หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒.๗ หน่วยงานควบคุมหรือกำกับดูแล

๒.๗.๑ ในขั้นตอนที่ ๑ กำกับดูแลการปฏิบัติของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การกำกับดูแลของตน ตามข้อ ๑.๑ ดังนี้

(๑) กำหนดมาตรฐานที่เหมาะสมเพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานของรัฐ

(๒) ตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตน

(๓) ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง (๔) ด้วย

๒.๗.๒ ในขั้นตอนที่ ๒ สนับสนุนการปฏิบัติตามข้อ ๑.๒ ดังนี้

(๑) รับรายงานเมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๒) รับแจ้งในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) เมื่อปรากฏแก่หน่วยงานควบคุมหรือกำกับดูแล หรือเมื่อหน่วยงานควบคุมหรือกำกับดูแลได้รับแจ้งเหตุตามมาตรา ๕๘ ให้หน่วยงานควบคุมหรือกำกับดูแล ร่วมกับหน่วยงานตาม

มาตรา ๕๐ รวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์

๒.๗.๓ ในขั้นตอนที่ ๓ สนับสนุนการปฏิบัติตามข้อ ๑.๓ ดังนี้

(๑) สนับสนุนและให้ความช่วยเหลือแก่หน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน และให้ความร่วมมือและประสานงานกับสำนักงาน ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

(๒) แจ้งเตือนหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน รวมทั้งหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอื่นที่เกี่ยวข้องโดยเร็ว

๒.๗.๔ ในขั้นตอนที่ ๔ สนับสนุนการปฏิบัติตามข้อ ๑.๔ ดังนี้

(๑) ร่วมกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การควบคุมหรือกำกับดูแลของตน นำเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและมีลักษณะเป็นภัยคุกคามทางไซเบอร์ที่มีนัยสำคัญมาเป็นกรณีศึกษา และหาแนวทางเพื่อเตรียมการรับมือและป้องกันการเกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะดังกล่าวร่วมกับบุคคลหรือหน่วยงานที่เกี่ยวข้อง

(๒) ร่วมกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การควบคุมหรือกำกับดูแลของตน ปรับปรุงมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับให้มีความเหมาะสม และเป็นปัจจุบัน

๒.๘ หน่วยงานของรัฐ

๒.๘.๑ ในขั้นตอนที่ ๑ ดำเนินการตามข้อ ๑.๑ ดังนี้

ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง (๔) ด้วย

๒.๘.๒ ในขั้นตอนที่ ๒ ดำเนินการตามข้อ ๑.๒ ดังนี้

(๑) ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐใด ให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่

(๒) หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้แจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว

๒.๘.๓ ในขั้นตอนที่ ๓ ดำเนินการตามข้อ ๑.๓ ดังนี้

หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น

๒.๘.๔ ในขั้นตอนที่ ๔ ดำเนินการตามข้อ ๑.๔

๒.๙ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒.๙.๑ ในขั้นตอนที่ ๑ ดำเนินการตามข้อ ๑.๑ ดังนี้

ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง (๔) ด้วย

๒.๙.๒ ในขั้นตอนที่ ๒ ดำเนินการตามข้อ ๑.๒ ดังนี้

(๑) ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่

(๒) หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้แจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว

(๓) เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศรายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในส่วนที่ ๔ ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

๒.๙.๓ ในขั้นตอนที่ ๓ ดำเนินการตามข้อ ๑.๓ ดังนี้

(๑) หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น

(๒) ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ดำเนินการตามคำสั่ง กกม.

๒.๙.๔ ในขั้นตอนที่ ๔ ดำเนินการตามข้อ ๑.๔

๒.๑๐ สภาความมั่นคงแห่งชาติ

๒.๑๐.๑ ในขั้นตอนที่ ๑ สนับสนุนการดำเนินการตามข้อ ๑.๑ ดังนี้

(๑) จัดทำแผนเตรียมพร้อมแห่งชาติ โดยให้ครอบคลุมภัยคุกคามทางไซเบอร์และมีความสอดคล้องกับ (ร่าง) แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕ – ๒๕๗๐ รวมถึง (ร่าง) แผนรับมือเหตุการณ์ทางไซเบอร์

(๒) จัดการฝึกการบริหารวิกฤตการณ์ระดับชาติ โดยให้ครอบคลุมภัยคุกคามทางไซเบอร์

๒.๑๐.๒ ในขั้นตอนที่ ๒ สนับสนุนการดำเนินการตามข้อ ๑.๒ ดังนี้

เมื่อได้รับแจ้ง และ/หรือรายงาน จาก สกมช. หรือในกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ให้ สมช. ยืนยันว่าเกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติหรือไม่

๒.๑๐.๓ ในขั้นตอนที่ ๓ สนับสนุนการดำเนินการตามข้อ ๑.๓ ดังนี้

ดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายว่าด้วยสภาความมั่นคงแห่งชาติและกฎหมายอื่นที่เกี่ยวข้อง

๒.๑๐.๔ ในขั้นตอนที่ ๔ สนับสนุนดำเนินการตามข้อ ๑.๔

ภาคผนวก

ผนวก ก

NCSA สกมช ด่วน

บันทึกข้อความ

หน่วยงาน สำนักบริหารโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (สบพ.) สกมช. โทร. ๐ ๒๑๔๒ ๖๘๘๘

ที่ สกมช ๐๖๐๐/๕๘ **วันที่** ๑๖ กันยายน ๒๕๖๔

เรื่อง ขออนุมัติจัดการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

เรียน ลธ.กมช.

๑. เรื่องเดิม

ตามที่ ลธ.กมช. ได้กรุณาอนุมัติให้ดำเนินการกิจกรรมจัดการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายในวงเงิน ๒,๔๙๗,๓๐๐.- บาท (สองล้านสี่แสนเก้าหมื่นเจ็ดพันสามร้อยบาทถ้วน) จากเงินงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ.๒๕๖๔ งบกลาง รายการเงินสำรองจ่ายเพื่อกรณีฉุกเฉินหรือจำเป็น รายละเอียดตามหนังสือ สงก. ด่วนที่สุด ที่ สกมช ๐๓๐๐/๑๙๒ ลงวันที่ ๑๘ สิงหาคม ๒๕๖๔ ที่แนบ ๑

๒. ข้อเท็จจริง

๒.๑ การดำเนินการในข้อ ๑ เป็นโครงการจ้างที่ปรึกษากิจกรรมจัดการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีวัตถุประสงค์ เพื่อให้หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีความรู้ความเข้าใจเกี่ยวกับการรับมือภัยคุกคามทางไซเบอร์ ตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

๒.๒ ขอบเขตของงาน (Terms of Reference : TOR) จ้างที่ปรึกษากิจกรรมจัดการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มี สบพ. เป็นผู้รับผิดชอบโครงการ ประกอบด้วยกิจกรรม ดังต่อไปนี้

๒.๒.๑ การประชุมพัฒนาแนวคิดการฝึก (Concept Development Conference: CDC) เพื่อออกแบบและพัฒนาแนวคิดการจัดการฝึก โดยสรุปประกอบด้วย วัตถุประสงค์ สถานการณ์ฝึกทั่วไป รูปแบบการฝึก ประเภทของโจทย์ฝึก หัวข้อสำหรับการฝึกเตรียมการ ระยะเวลาการดำเนินงาน โครงสร้างการฝึก รวมถึงรายชื่อหน่วยงานและจำนวนคนที่จะเข้าร่วมการฝึกในขั้นต้น

๒.๒.๒ การประชุมวางแผนขั้นต้น (Initial Planning Conference: IPC) เพื่อกำหนดวัตถุประสงค์ สถานการณ์ฝึกทั่วไป รูปแบบการฝึก ประเภทของโจทย์ฝึก ระยะเวลาการดำเนินงาน โครงสร้างการฝึก และรายชื่อผู้ติดต่อประสานหน่วยงานที่จะเข้ารับการฝึก

๒.๒.๓ การประชุมจัดทำสถานการณ์ฝึก (Scenario and Inject Development) เพื่อจัดทำสถานการณ์ฝึกทั่วไป สถานการณ์ฝึกเฉพาะ โจทย์ฝึกและผลลัพธ์ที่คาดหวัง รวมถึงหัวข้อสำหรับการฝึกเตรียมการ

๒.๒.๔ การประชุมวางแผนขั้นสุดท้าย (Final Planning Conference: FPC) เพื่อยืนยันวัตถุประสงค์ สถานการณ์ฝึกทั่วไป สถานการณ์ฝึกเฉพาะ รูปแบบการฝึก โจทย์หรือประเภทของโจทย์ฝึก หัวข้อสำหรับการฝึกเตรียมการ ระยะเวลาการดำเนินงาน โครงสร้างการฝึก รายชื่อผู้ติดต่อประสานหน่วยงานที่จะเข้ารับการฝึก รายชื่อหน่วยงานและจำนวนคนที่จะเข้าร่วมการฝึก ตลอดจนบทบาทและความรับผิดชอบของผู้ที่เกี่ยวข้อง

๒.๒.๕ การฝึกเตรียมการ (Pre-exercise/Academic) เพื่อเสริมสร้างความเข้าใจและพัฒนาศักยภาพของหน่วยงานของรัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานควบคุมหรือกำกับดูแล ให้มีความพร้อมก่อนที่จะเข้าร่วมการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ (Staff-Exercise : Staff-Ex)

/๒.๒.๖ การฝึก ...

๒.๒.๖ การฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ (Staff-Exercise : Staff-Ex) ในรูปแบบการฝึกซ้อมแผนบนโต๊ะ (Table Top Exercise: TTX) โดยใช้การรวมกลุ่มอภิปรายเพื่อแก้ไขปัญหาตามโจทย์ฝึกและสถานการณ์ฝึกที่กำหนด โดยมีส่วนควบคุมการฝึก (Exercise Control Group : ECG) เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามแนวทางและวัตถุประสงค์ของการฝึก รวมทั้งกำหนดให้มีส่วนประเมินผลการฝึก (Exercise Evaluation Group : EEG) เป็นผู้รับผิดชอบการประเมินผลผู้รับการฝึกด้วย

๓. ข้อพิจารณา

เพื่อให้การจัดการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นไปด้วยความเรียบร้อย สบพ. พิจารณาแล้ว เห็นควรกำหนดให้มีโครงสร้างและการแบ่งมอบความรับผิดชอบ กำหนดการฝึก และเนื้อหาสำหรับการประชุมวางแผนการฝึก ดังนี้

๓.๑ โครงสร้างและการแบ่งมอบความรับผิดชอบ ตามแนบ ๒

๓.๒ กำหนดการฝึก ตามแนบ ๓

๓.๓ เนื้อหาสำหรับการประชุมวางแผนการฝึก ตามแนบ ๔

๔. ข้อเสนอ เห็นควรดำเนินการ ดังนี้

๔.๑ อนุมัติให้ สบพ. จัดการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามโครงสร้างและการแบ่งมอบความรับผิดชอบ กำหนดการฝึก และเนื้อหาสำหรับการประชุมวางแผนการฝึก ในข้อ ๓

๔.๒ แจ้งให้ ศูนย์/สำนัก ทราบและปฏิบัติตามการอนุมัติในข้อ ๔.๑

๔.๓ กรุณาตอบรับเป็นผู้อำนวยการ กองอำนวยการฝึก ตามโครงสร้างและการแบ่งมอบความรับผิดชอบ ในข้อ ๓.๑ และประธานกิจกรรมตามข้อ ๒.๒.๑ - ๒.๒.๖ หากติดภารกิจกรุณากำหนดผู้แทน

๔.๔ หากมีการเปลี่ยนแปลงกำหนดการฝึกโดยงบประมาณไม่เพิ่มขึ้น ให้ สบพ. สามารถดำเนินการได้ตามความเหมาะสม

จึงเรียนมาเพื่อกรุณาพิจารณาให้ความเห็นชอบ ลงนามในหนังสือเชิญหน่วยงาน และอนุมัติให้ใช้ลายมือชื่ออิเล็กทรอนิกส์ในหนังสือถึงหน่วยงานตามรายชื่อแนบท้าย

น.อ.

(จเด็ด คูหะก้องกิจ)
ปฏิบัติหน้าที่ ผอ.สบพ.

อนุมัติในข้อ ๔

- ลงนามแล้ว
พล.ท.

(ปรัชญา เฉลิมวัฒน์)
ลธ.กมช.
๑๗ ก.ย. ๒๕๖๔

น.อ.

(อมร ชมเชย)
ปฏิบัติหน้าที่ รอง ลธ.กมช.

ผนวก ข

๑/๑๑/๒๐๒๑

ระเบียบคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
ว่าด้วยการมอบอำนาจ และการกำหนดให้หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐาน
สำคัญทางสารสนเทศที่ถูกคุกคามเข้าร่วมดำเนินการ ประสานงาน และให้การสนับสนุน
ในการปฏิบัติการเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์
พ.ศ. ....

โดยที่เป็นการสมควรกำหนดให้มีระเบียบและวิธีปฏิบัติเกี่ยวกับการมอบอำนาจ และการกำหนดให้หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ถูกคุกคามเข้าร่วมดำเนินการ ประสานงาน และให้การสนับสนุน ในการปฏิบัติการเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์ เพื่อให้มีการรับมือกับภัยคุกคามทางไซเบอร์ได้ทันท่วงที

อาศัยอำนาจตามความในมาตรา ๑๔ วรรคสอง แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบมติที่ประชุมคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ครั้งที่ ../๒๕๖๔ เมื่อวันที่ ..... คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์จึงออกระเบียบไว้ ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ว่าด้วยการมอบอำนาจ และการกำหนดให้หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ถูกคุกคามเข้าร่วมดำเนินการ ประสานงาน และให้การสนับสนุน ในการปฏิบัติการเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์ พ.ศ. ....”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ในระเบียบนี้

“กกม.” หมายความว่า คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

“ประธาน กกม.” หมายความว่า ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

“คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์” หมายความว่า คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ด้านต่าง ๆ ที่ได้รับมอบอำนาจจากคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อร่วมกันปฏิบัติการในเรื่องการดูแลและดำเนินการ และรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“เลขาธิการ” หมายความว่า เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ข้อ ๔ ให้มีคณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ ประกอบด้วย

(๑) รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ

(๒) ผู้บัญชาการทหารสูงสุด เป็นกรรมการ

(๓) ผู้บัญชาการตำรวจแห่งชาติ เป็นกรรมการ

(๔) เลขาธิการ เป็นกรรมการและเลขานุการ

ให้เลขาธิการแต่งตั้งพนักงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

ข้อ ๕ คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ มีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) ร่วมกันปฏิบัติการเพื่อรับมือกับภัยคุกคามทางไซเบอร์

(๒) ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ตามมาตรา ๖๑ มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ มาตรา ๖๕ และมาตรา ๖๖ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๒

(๓) ปฏิบัติการอื่นใดตามที่ กกม. มอบหมาย

ข้อ ๖ การประชุมของคณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ ให้นำระเบียบคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยการประชุมของคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ และคณะอนุกรรมการ มาใช้บังคับโดยอนุโลม

ข้อ ๗ เมื่อคณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ ดำเนินการตามข้อ ๕ แล้วให้รายงานผลการดำเนินการดังกล่าว ต่อ กกม. ทราบด้วย

ข้อ ๘ ให้หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ถูกคุกคามเข้าร่วมดำเนินการ ประสานงาน และให้การสนับสนุน ต่อคณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ เพื่อรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที

ข้อ ๙ ให้ประธาน กกม. เป็นผู้รักษาการตามระเบียบนี้ และมีอำนาจออกประกาศ หรือคำสั่ง

ในกรณีที่มีปัญหาเกี่ยวกับการบังคับใช้หรือการปฏิบัติตามระเบียบนี้ หรือระเบียบนี้ไม่ได้กำหนดเรื่องใดไว้ ให้ประธาน กกม. มีอำนาจตีความและวินิจฉัยชี้ขาด แล้วรายงานให้ กกม. ทราบ ทั้งนี้ การตีความและคำวินิจฉัยของประธาน กกม. ให้เป็นที่สุด

ประกาศ ณ วันที่ เดือน พ.ศ. ๒๕๖๔

(นายชัยวุฒิ ธนาคมานุสรณ์)

รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

ผนวก ค

หน้า ๓
เล่ม ๑๓๘ ตอนพิเศษ ๓๐๓ ง ราชกิจจานุเบกษา ๑๑ ธันวาคม ๒๕๖๔

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

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

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประกาศกำหนดรายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ

อาศัยอำนาจตามความในมาตรา ๖๐ วรรคสอง แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๒/๒๕๖๔ ลงวันที่ ๔ ตุลาคม ๒๕๖๔ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ เพื่อประโยชน์ในการจำแนกลักษณะของภัยคุกคามทางไซเบอร์แต่ละระดับ ให้กำหนดรายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และภัยคุกคามทางไซเบอร์ในระดับวิกฤต โดยพิจารณาและประเมินจากระดับผลกระทบที่อาจเกิดขึ้นหากระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือระบบงานที่มีความสำคัญอื่น ๆ ถูกโจมตีจากภัยคุกคามทางไซเบอร์ ตามลักษณะและการประเมินภัยคุกคามทางไซเบอร์แต่ละระดับที่กำหนดในเอกสารแนบ ๑ ท้ายประกาศนี้

ข้อ ๔ เพื่อให้การดำเนินการรับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์เป็นไปอย่างเหมาะสมและสอดคล้องกับลักษณะของภัยคุกคามทางไซเบอร์แต่ละระดับ ให้กำหนดแนวทางที่เกี่ยวข้อง เพื่อเป็นข้อเสนอแนะสำหรับการจัดการกับภัยคุกคามทางไซเบอร์ ตามหลักเกณฑ์ เงื่อนไข และวิธีการที่กำหนดในเอกสารแนบ ๒ ท้ายประกาศนี้

ข้อ ๕ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ รักษาการตามประกาศนี้

หน้า ๔
เล่ม ๑๓๘ ตอนพิเศษ ๓๐๓ ง ราชกิจจานุเบกษา ๑๑ ธันวาคม ๒๕๖๔

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เป็นผู้มีอำนาจตีความและวินิจฉัยชี้ขาด การตีความและคำวินิจฉัยของประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๒๕ พฤศจิกายน พ.ศ. ๒๕๖๔
พลเอก ประวิตร วงษ์สุวรรณ
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เอกสารแนบ ๑ ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม
และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔
ว่าด้วยลักษณะและการประเมินภัยคุกคามทางไซเบอร์แต่ละระดับ

บทนำ

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น ๓ ระดับ ได้แก่ ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และภัยคุกคามทางไซเบอร์ในระดับวิกฤติ โดยได้มีการให้ความหมายของภัยคุกคามทางไซเบอร์ในแต่ละระดับไว้แล้วนั้น เพื่อให้เกิดความสะดวกแก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการประเมินและระบุระดับของภัยคุกคามทางไซเบอร์ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงได้กำหนดลักษณะและการประเมินภัยคุกคามทางไซเบอร์แต่ละระดับโดยพิจารณาจากปัจจัยต่าง ๆ เพื่อเป็นแนวทางให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สำหรับการพิจารณาระบุระดับของภัยคุกคามทางไซเบอร์ ดังมีรายละเอียดปรากฏตามแนบท้ายนี้

นิยาม

๑.	คณะกรรมการ	หมายถึง	คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๒.	บริการหลัก	หมายถึง	ภารกิจหรือบริการอันถือเป็นหน้าที่โดยตรงของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งมีการดำเนินภารกิจหรือให้บริการโดยใช้ระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ ในการดำเนินการ
๓.	โครงสร้างสำคัญทางสารสนเทศ	หมายถึง	โครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่เกี่ยวข้องกับความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความสงบเรียบร้อยของประชาชน ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ
๔.	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์	หมายถึง	การกระทำโดยมิชอบที่มีผลต่อคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ โดยทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์แล้วแต่กรณี เสียหาย ถูกทำลาย ด้อยประสิทธิภาพหรือไม่สามารถนำมาใช้งานได้ และให้หมายความรวมถึงการกระทำอื่นใดที่มีผลในทำนองเดียวกัน
๕.	ข้อมูล	หมายถึง	ข้อความ ข้อเท็จจริง หรือโปรแกรมที่มีการสร้าง จัดเก็บ หรือมีการใช้งาน โดยสามารถรับ-ส่งด้วยซอฟต์แวร์คอมพิวเตอร์ รวมถึงซอฟต์แวร์ระบบ โปรแกรมประยุกต์ หรือสื่ออื่นใดที่ใช้คู่กับอุปกรณ์คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ที่ถูกควบคุมด้วยอิเล็กทรอนิกส์ ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ

๖. การประทุษร้ายต่อข้อมูล	หมายถึง	การกระทำโดยมิชอบที่มีผลเป็นการเปลี่ยนแปลงข้อมูล ทำลายข้อมูล ขโมยข้อมูล นำข้อมูลไปใช้โดยไม่ได้รับอนุญาต หรือจำกัดมิให้ผู้เป็นเจ้าของหรือผู้ครอบครองข้อมูลเข้าถึงข้อมูลของตนได้ และให้หมายความรวมถึงการกระทำอื่นใดที่มีผลในทำนองเดียวกัน
๗. แผนการกู้คืน	หมายถึง	แผนปฏิบัติงานหรือรายละเอียดความตกลงที่เกี่ยวข้องกับการกู้คืนระบบหรือการกู้คืนการให้บริการ (service level agreement) หรือ แผนการบริหารความต่อเนื่องของหน่วยงาน แล้วแต่กรณี
๘. มาตรการเร่งด่วน	หมายถึง	มาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัดหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

ลักษณะของภัยคุกคามทางไซเบอร์ และปัจจัยที่ใช้ในการประเมินภัยคุกคามทางไซเบอร์แต่ละระดับ

ในการพิจารณาระบุระดับของภัยคุกคามทางไซเบอร์ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรพิจารณาจากเหตุการณ์ต่าง ๆ ที่เป็นพฤติการณ์แวดล้อม ผลกระทบที่เกิดขึ้น ความเสี่ยงหรือแนวโน้มที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์ในกรณีต่าง ๆ เพื่อพิจารณาว่าลักษณะของภัยคุกคามทางไซเบอร์นั้นอยู่ในระดับใด โดยให้พิจารณาจากปัจจัยที่ใช้ในการประเมินทั้ง ๔ ปัจจัย ดังนี้

(๑) ลักษณะผลกระทบที่เกิดขึ้นต่ออุปกรณ์หรือระบบงาน

(๒) ลักษณะผลกระทบต่อข้อมูลในระบบ

(๓) แนวโน้มในการกู้คืนระบบ

(๔) ลักษณะผลกระทบต่อลูกค้าหรือผู้ใช้บริการ

การพิจารณาเพื่อระบุระดับของภัยคุกคามทางไซเบอร์แต่ละระดับนั้น หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรพิจารณาให้ครบทั้ง ๔ ปัจจัย ตามที่ได้ระบุไว้ข้างต้น โดยหากปรากฏข้อเท็จจริงว่าลักษณะภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้นเข้าลักษณะหรือมีแนวโน้มเป็นภัยคุกคามทางไซเบอร์ในระดับใด ให้ถือเอาระดับสูงสุดที่ประเมินได้เป็นเกณฑ์ในการระบุระดับของภัยคุกคามทางไซเบอร์ในครั้งนั้น ๆ นอกจากนี้ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอาจพิจารณากำหนดปัจจัยที่ใช้ในการประเมินและลักษณะภัยคุกคามทางไซเบอร์เพิ่มเติมร่วมกับหน่วยงานควบคุมหรือกำกับดูแลเพื่อให้มีแนวทางในการจำแนกระดับของภัยคุกคามทางไซเบอร์ที่เหมาะสม โดยจะต้องมีรายละเอียดไม่น้อยกว่าหรือเทียบเท่ากับแนวทางการพิจารณาที่กำหนดไว้ในตารางที่ ๑

อย่างไรก็ดี เพื่อให้การดำเนินการรับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับมีความเหมาะสมและสอดคล้องกับสถานการณ์โดยรวมที่เกิดขึ้น คณะกรรมการอาจพิจารณาปรับเปลี่ยนหรือยกระดับของภัยคุกคามทางไซเบอร์ที่ได้รับรายงานเป็นอย่างอื่นได้ หากปรากฏข้อเท็จจริงเพิ่มเติมหรือพบว่าภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้นมีแนวโน้มที่จะลุกลามหรือก่อให้เกิดความเสียหายมากขึ้น

อนึ่ง เพื่อให้สอดคล้องกับสภาวการณ์ที่เปลี่ยนแปลงไป คณะกรรมการหรือผู้ที่ได้รับมอบหมายจากคณะกรรมการอาจพิจารณาทบทวนลักษณะภัยคุกคามทางไซเบอร์ ปรับปรุงปัจจัยที่ใช้ในการประเมินหรือนำเงื่อนไขอื่น ๆ มาประกอบการพิจารณาเพิ่มเติมได้ตามที่เห็นสมควร

ตารางที่ ๑ ลักษณะภัยคุกคามทางไซเบอร์แต่ละระดับและแนวทางการพิจารณาผลกระทบ

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์	
	ระดับไม่ร้ายแรง	ระดับร้ายแรง
๑. ลักษณะผลกระทบที่เกิดขึ้นต่ออุปกรณ์หรือระบบงาน	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ดังนี้ (๑) ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือ (๒) อุปกรณ์หรือระบบงานอื่นใดที่ใช้สำหรับการให้บริการของรัฐ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าว ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือการให้บริการของรัฐด้อยประสิทธิภาพลงไปบ้าง แต่ไม่ถึงขนาดที่จะทำให้ระบบหรือบริการต้องหยุดชะงักหรือไม่สามารถใช้งานได้	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่ถูกใช้สำหรับให้บริการหลัก ดังนี้ (๑) ระบบคอมพิวเตอร์ (๒) โครงสร้างสำคัญทางสารสนเทศ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าว แสดงให้เห็นได้ว่าผู้โจมตีมีความมุ่งหมายที่จะทำให้โครงสร้างพื้นฐานสำคัญของประเทศเสียหายจนไม่สามารถทำงานหรือให้บริการได้

ลักษณะภัยคุกคามทางไซเบอร์	
ระดับวิกฤติ	
กรณี (ก)	กรณี (ข)
การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่รุนแรงในลักษณะที่เป็นวงกว้างต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าว ทำให้ (๑) การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบจนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือ (๒) การใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ	ไม่เจาะจงอุปกรณ์หรือระบบงานที่ได้รับผลกระทบ แต่เมื่อพิจารณาจากพฤติกรรมของผู้โจมตีหรือพฤติการณ์แวดล้อมแล้วมีเหตุอันควรเชื่อได้ว่าการก่อภัยคุกคามทางไซเบอร์นั้นกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์	
	ระดับไม่ร้ายแรง	ระดับร้ายแรง
๒. ลักษณะผลกระทบต่อข้อมูลในระบบ	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูล ซึ่งส่งผลกระทบทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือการให้บริการของรัฐด้อยประสิทธิภาพลงไปบ้าง แต่ไม่ถึงขนาดที่จะทำให้ระบบหรือบริการต้องหยุดชะงักหรือไม่สามารถใช้งานได้	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลที่ใช้สำหรับระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศ ซึ่งส่งผลให้บริการหลักไม่สามารถทำงานหรือให้บริการได้
๓. แนวโน้มในการกู้คืนระบบ	สามารถกู้คืนระบบคอมพิวเตอร์ หรือทำให้บริการของรัฐกลับมาได้บางส่วน โดยสามารถดำเนินการได้ตามแผนการกู้คืน	ไม่สามารถกู้คืนระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่ใช้สำหรับให้บริการหลักได้ ตามแผนการกู้คืน

ลักษณะภัยคุกคามทางไซเบอร์	
ระดับวิกฤติ	
กรณี (ก)	กรณี (ข)
มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลอันมีลักษณะดังนี้ (๑) เป็นข้อมูลที่เกี่ยวข้องกับการทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชน หรือ (๒) เป็นข้อมูลที่เกี่ยวข้องกับชีวิตของบุคคลจำนวนมาก หรือเป็นข้อมูลคอมพิวเตอร์จำนวนมากในระดับประเทศ	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลใด ๆ อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม
ไม่สามารถกู้คืนการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศได้ตามแผนการกู้คืน ทำให้ (๑) รัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือ (๒) มีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิต หรือระบบคอมพิวเตอร์ คอมพิวเตอร์ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ	ไม่สามารถกู้คืนอุปกรณ์หรือระบบงานที่ได้รับผลกระทบได้ และจำเป็นต้องมีมาตรการเร่งด่วนในการกู้คืนอุปกรณ์หรือระบบงานที่เกี่ยวข้อง

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์	
	ระดับไม่ร้ายแรง	ระดับร้ายแรง
๔. ลักษณะผลกระทบต่อลูกค้าหรือผู้ใช้บริการ	ส่งผลหรืออาจส่งผลกระทบต่อผู้ใช้บริการในวงจำกัด	อาจส่งผลกระทบต่อผู้ใช้บริการทั้งหมด

ลักษณะภัยคุกคามทางไซเบอร์	
ระดับวิกฤติ	
กรณี (ก)	กรณี (ข)
ส่งผลกระทบต่อผู้ใช้บริการทั้งหมด หรือ อาจมีผลทำให้บุคคลจำนวนมากเสียชีวิต	ส่งผลหรืออาจส่งผลกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม

๖

เอกสารแนบ ๒ ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม
และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔
ว่าด้วยมาตรการป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ

บทนำ

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น ๓ ระดับ ได้แก่ ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และภัยคุกคามทางไซเบอร์ในระดับวิกฤติ นั้น

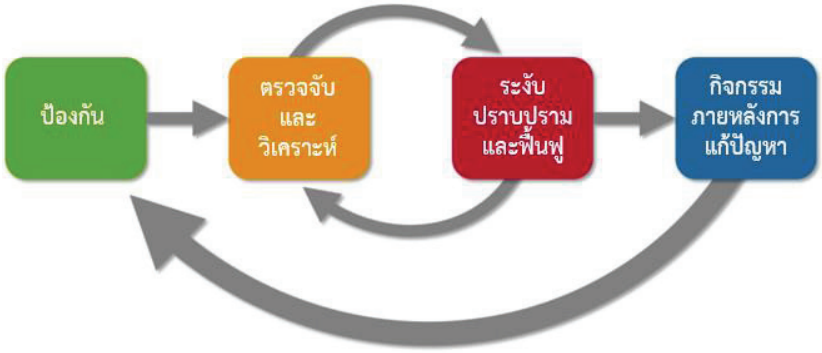
เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือหน่วยงานที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ มีแนวทางปฏิบัติที่ชัดเจนในการดำเนินมาตรการป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงกำหนดรายละเอียดที่เกี่ยวข้องเพื่อเป็นแนวทางดำเนินการไว้ในแนบท้ายนี้

นิยาม

๑. ทรัพย์สินสำคัญทางสารสนเทศ	หมายถึง	ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือระบบงานที่มีความสำคัญอื่น ๆ ตามที่หน่วยงานพิจารณาแล้วเห็นว่ามีความจำเป็นต้องเฝ้าระวัง หรือดำเนินมาตรการป้องกัน รับมือ และแก้ไขภัยคุกคามทางไซเบอร์
๒. หน่วยงาน	หมายถึง	หน่วยงานหรือองค์กรที่มีการครอบครองหรือเป็นเจ้าของทรัพย์สินสำคัญทางสารสนเทศ ซึ่งอาจได้รับผลกระทบหากมีภัยคุกคามทางไซเบอร์เกิดขึ้น
๓. แนวปฏิบัติพื้นฐาน (Security Control Baselines)	หมายถึง	แนวปฏิบัติพื้นฐานที่กำหนดไว้สำหรับการดำเนินมาตรการป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ

มาตรการป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ

การดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์ (incident handling) นั้น สามารถแบ่งขั้นตอนการดำเนินการออกได้เป็น ๔ ขั้นตอนหลัก เพื่อให้สอดคล้องกับมาตรฐานหรือแนวทางปฏิบัติสากลที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดดังนี้



ภาพแสดงขั้นตอนการดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์
(Incident Handling Cycle)

ขั้นตอนที่ ๑: การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์

การดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ โดยพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุในตารางที่ ๒.๑

ขั้นตอนที่ ๒: การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์

แม้ว่าหน่วยงานจะจัดให้มีมาตรการต่าง ๆ เพื่อป้องกันหรือควบคุมมิให้เกิดภัยคุกคามทางไซเบอร์ขึ้นแล้วก็ตาม แต่หน่วยงานก็ยังคงต้องเตรียมความพร้อมอยู่เสมอเพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจหลีกเลี่ยงได้ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) จึงเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุในตารางที่ ๒.๒

๘

ขั้นตอนที่ ๓: การระงับภัยคุกคามทางไซเบอร์[๑] ปราบปรามภัยคุกคามทางไซเบอร์[๒] และการฟื้นฟูระบบงานที่ได้รับผลกระทบ[๓]

เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือเมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานควรกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery) โดยการดำเนินการดังกล่าว ควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ โดยพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุในตารางที่ ๒.๓ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป

ขั้นตอนที่ ๔: การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity) นั้น หน่วยงานควรกำหนดขั้นตอน วิธีปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน โดยพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุในตารางที่ ๒.๔ ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง (โดยการเก็บข้อมูลบางประเภทนั้นอาจจำเป็นต้องดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไปในระหว่างที่ต้องระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตี)

เมื่อมีการเก็บรวบรวมข้อมูลและหลักฐานที่จำเป็นตามวรรคหนึ่งแล้ว หน่วยงานควรนำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคามทางไซเบอร์ โดยอาจจัดทำเป็นรายสัปดาห์หรือรายเดือน เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน และกำหนดขั้นตอนที่หน่วยงานควรดำเนินการ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ในลักษณะดังกล่าวขึ้นอีกในอนาคต

---

[๑] การระงับภัยคุกคามทางไซเบอร์ คือ การดำเนินการเพื่อจำกัดความเสียหายจากภัยคุกคามทางไซเบอร์ที่กำลังเกิดขึ้น กักกันภัยคุกคามไม่ให้แพร่กระจาย และป้องกันไม่ให้มีความเสียหายเพิ่มมากขึ้น โดยผู้เผชิญเหตุภัยคุกคามทางไซเบอร์ต้องระมัดระวังไม่ให้หลักฐานทางนิติวิทยาศาสตร์ถูกทำลายในการดำเนินการดังกล่าว

[๒] การปราบปรามภัยคุกคามทางไซเบอร์ คือ การดำเนินการกำจัดภัยคุกคาม ผู้เผชิญเหตุภัยคุกคามทางไซเบอร์จะต้องลบโปรแกรมหรือสิ่งที่ไม่พึงประสงค์ (malicious object) ออกให้หมด และตรวจสอบระบบที่ได้รับผลกระทบทั้งระบบเพื่อให้มั่นใจถึงความปลอดภัยด้านไซเบอร์ โดยพยายามให้เกิดความเสียหายต่อข้อมูลน้อยที่สุด

[๓] การฟื้นฟูระบบงานที่ได้รับผลกระทบ คือ การดำเนินการเพื่อนำระบบให้กลับมาอยู่ในสถานะปกติที่มั่นใจว่าปราศจากการโจมตีที่เป็นภัยคุกคามทางไซเบอร์ โดยรวมถึงการเฝ้าระวังและตรวจสอบระบบที่ถูกกู้คืนในระยะแรกของการนำกลับมาใช้งาน เพื่อป้องกันการโจมตีซ้ำ

๙

อนึ่ง ในการป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์ ตามรายละเอียดที่ระบุไว้ข้างต้นนั้น หน่วยงานควรจัดให้มีมาตรการที่สอดคล้องกับระดับของภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงานนั้น ๆ โดยให้ใช้แนวทางการประเมินความเสี่ยงของหน่วยงานเป็นเกณฑ์ในการพิจารณา ประกอบกับความสำคัญของภารกิจหรือบริการที่อยู่ภายใต้ความรับผิดชอบของหน่วยงาน ความสำคัญของทรัพย์สินสำคัญทางสารสนเทศ และอาจนำปัจจัยที่ใช้ในการประเมินระดับภัยคุกคามทางไซเบอร์ ตามตารางที่ ๑ ของเอกสารแนบ ๑ มาประกอบการพิจารณาด้วยก็ได้ นอกจากนี้ หน่วยงานอาจพิจารณากำหนดแนวทางการดำเนินมาตรการต่าง ๆ เพิ่มเติมหรือแตกต่างจากที่กำหนดไว้ เพื่อป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์ หรือจัดทำนโยบายที่เกี่ยวข้องร่วมกับหน่วยงานควบคุมหรือกำกับดูแลเพื่อให้มีแนวทางการดำเนินมาตรการที่เหมาะสม โดยจะต้องมีรายละเอียดไม่น้อยกว่าหรือเทียบเท่ากับมาตรการต่าง ๆ ที่กำหนดไว้ในแนบท้ายนี้

รายละเอียดที่เกี่ยวข้องเพื่อเป็นแนวทางในการดำเนินมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้กำหนดรายละเอียดที่เกี่ยวข้องเพื่อเป็นแนวทางในการดำเนินมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับไว้ ดังนี้

๑. กรณีหน่วยงานมีการครอบครองทรัพย์สินสำคัญทางสารสนเทศที่อาจมีแนวโน้มนำไปสู่ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง

ให้หน่วยงานพิจารณาดำเนินมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์ ตามแนวทางที่ระบุในประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานซึ่งได้จัดทำขึ้นตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และที่แก้ไขเพิ่มเติม (ถ้ามี) และดำเนินการตามแนวปฏิบัติพื้นฐาน (Security Control Baselines) ที่กำหนดไว้ในตารางที่ ๒.๑ – ตารางที่ ๒.๔ (สำหรับกรณีภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง)

๒ กรณีหน่วยงานมีการครอบครองทรัพย์สินสำคัญทางสารสนเทศที่อาจมีแนวโน้มนำไปสู่ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

ให้หน่วยงานพิจารณาดำเนินมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์ ตามแนวทางที่ระบุในข้อ ๑ และดำเนินการตามแนวปฏิบัติพื้นฐาน (Security Control Baselines) ที่กำหนดไว้เพิ่มเติมในตารางที่ ๒.๑ – ๒.๔ (สำหรับกรณีภัยคุกคามทางไซเบอร์ในระดับร้ายแรง)

๓ กรณีหน่วยงานมีการครอบครองทรัพย์สินสำคัญทางสารสนเทศที่อาจมีแนวโน้มนำไปสู่ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ

ให้หน่วยงานพิจารณาดำเนินมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์ ตามแนวทางที่ระบุในข้อ ๒ และดำเนินการตามแนวปฏิบัติพื้นฐาน (Security Control Baselines) ที่กำหนดไว้เพิ่มเติมในตารางที่ ๒.๑ – ๒.๔ (สำหรับกรณีภัยคุกคามทางไซเบอร์ในระดับวิกฤติ)

ตารางที่ ๒.๑ การดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	(๑) จัดเตรียมข้อมูลและอุปกรณ์การติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อของบุคคลหรือองค์กรต่าง ๆ คู่มือการปฏิบัติงานเพื่อรับมือกับภัยคุกคามทางไซเบอร์ และกลไกอื่นใด ที่ช่วยสนับสนุนการรายงานเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น เป็นต้น (๒) จัดเตรียมอุปกรณ์หรือทรัพยากรสนับสนุนที่จำเป็นสำหรับการรับมือกับภัยคุกคามทางไซเบอร์ (๓) ดำเนินการให้มีการจัดหมวดหมู่ข้อมูลและระบบสารสนเทศให้สอดคล้องกับแนวทางของกฎหมาย กฎเกณฑ์ หรือนโยบายต่าง ๆ ที่เกี่ยวข้อง เพื่อธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) ตลอดจนสภาพพร้อมใช้งาน (availability) ของข้อมูลและระบบสารสนเทศดังกล่าว (๔) จัดเตรียมข้อมูลสนับสนุนที่จำเป็นสำหรับการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ เช่น รายการทรัพย์สินสำคัญทางสารสนเทศ และแผนผังโครงสร้างเครือข่าย (Network diagrams) เป็นต้น (๕) พิจารณาช่อนบริการหรือระบบที่ผู้โจมตีสามารถค้นพบในเครือข่ายได้ง่าย โดยไม่ต้องใช้ความพยายามเจาะระบบ เช่น การค้นหาผ่านกลไกการสืบค้น (discovery protocol) เป็นต้น (๖) ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configura-tionchange control) และจัดทำแผนการบริหารจัดการการตั้งค่าหรือการเปลี่ยนแปลงค่าของอุปกรณ์ (configuration management plan) (๗) กำหนดตัวบุคคลหรือมอบหมายให้เจ้าหน้าที่ที่มีความชำนาญเป็นผู้ดำเนินการที่เกี่ยวข้องกับการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ รวมถึงการทำหน้าที่ในการประสานงานหรือหารือกับผู้ที่เกี่ยวข้อง (๘) จัดให้มีกระบวนการในการพิสูจน์ตัวตนผู้ใช้งานก่อนทางการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ใด ๆ เช่น การเข้ารหัสข้อมูลและการบริหารจัดการคีย์สำหรับการเข้าถึงระบบต่าง ๆ (cryptography / key managements) เป็นต้น (๙) ตรวจสอบแอปพลิเคชันที่ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความปลอดภัยเพียงพอ โดยมีการคัดกรองนักพัฒนา (developer screening) ที่ได้รับมอบหมายให้ดำเนินการใด ๆ กับเครือข่าย แอปพลิเคชัน หรือระบบงานต่าง ๆ (๑๐) ดำเนินการให้มีการทดสอบความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ (incident respond capability testing) (๑๑) รวบรวมข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ (threat Intelligence)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	(๑๓) กำหนดแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์ (๑๔) ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control) และจัดทำแผนการบริหารจัดการการตั้งค่าหรือการเปลี่ยนแปลง ค่าของอุปกรณ์ (configuration management plan) โดยจะต้องจัดให้มีกลไกที่สามารถบันทึกประวัติการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ที่เป็นลายลักษณ์อักษร การแจ้งเตือนเมื่อมีการเปลี่ยนแปลงค่าของอุปกรณ์ที่ตั้งไว้ และให้พิจารณาจัดให้มีกลไกที่สามารถป้องกันการเปลี่ยนแปลงค่าของอุปกรณ์ต่าง ๆ โดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม) (๑๕) จัดให้มีการฝึกอบรมเพื่อเตรียมพร้อมรับมือกับสถานการณ์ฉุกเฉินเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น (simulated events) เพื่อให้ผู้ปฏิบัติรับทราบบทบาทและความรับผิดชอบของตนเมื่อต้องรับมือกับสถานการณ์ดังกล่าว (๑๖) สร้างเครือข่ายความร่วมมือเพื่อแบ่งปันข้อมูลและประสานงานเกี่ยวกับการจัดการภัยคุกคามทางไซเบอร์

ตารางที่ ๒.๒ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	(๑) จัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสาคัญทางสารสนเทศ เป็นต้น (๒) จัดให้มีกลไกที่สามารถรับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ (๓) จัดให้มีข้อพึงปฏิบัติพื้นฐานเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อความการแจ้งข้อผิดพลาด หรือข้อความเตือนภัยจากเครื่องมือรักษาความปลอดภัยด้านไซเบอร์ และการตรวจสอบระบบงานที่มีความสำคัญ (critical systems) โดยจะต้องจัดให้มีข้อพึงปฏิบัติที่สูงขึ้นสำหรับทุกระบบงานที่มีความสำคัญมากขึ้น (๔) วิเคราะห์ข้อมูลและประวัติการใช้งานต่าง ๆ เช่น ลักษณะการใช้งานเครือข่ายและระบบงาน (profile networks and systems) เป็นต้น เพื่อทำความเข้าใจพฤติกรรมการใช้งานในช่วงเวลาปกติ (normal behaviors) ทางการศึกษาวิจัยและค้นหาความสัมพันธ์ของข้อมูลในระบบกับสถานการณ์ต่าง ๆ (event correlation) (๕) ทันทีที่พบว่ามี หรืออาจมีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการสืบหาและรวบรวมข้อมูลทั้งหมด เช่น ลักษณะภัยคุกคามทางไซเบอร์, ช่องโหว่ที่อาจถูกใช้ในการโจมตี, สถานการณ์ของการโจมตี (อาทิ กำลังเกิดเหตุหรือสถานการณ์ได้สิ้นสุดแล้ว การโจมตีเป็นผลสำเร็จหรือไม่สำเร็จ ฯลฯ) จำนวนระบบหรือบริการที่ได้รับผลกระทบ, โฮสต์เนม ตำแหน่งหรือสถานที่ของระบบหรือบริการที่ได้รับผลกระทบ ข้อมูลผู้ใช้ เวลาประทับ ข้อมูล payload ข้อมูลแจ้งเตือนจาก IDS (ถ้ามี) และ ข้อมูลจราจรทางคอมพิวเตอร์ (log) เป็นต้น โดยหน่วยงานจะต้องเก็บรักษาข้อมูลดังกล่าว (safeguardincident data) ให้มีความปลอดภัย เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้ เป็นพยานหลักฐานในการดำเนินคดี รวมถึงการจัดทำรายงานที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ (๖) ระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ตามสถานการณ์ที่เกิดขึ้น และติดตามเพื่อระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไปจนกว่าสถานการณ์ดังกล่าวจะสิ้นสุด โดยอาจพิจารณาจากข้อมูลตามที่ระบุในข้อ ๒ ของภาคผนวกแนบท้ายนี้

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	(๗) จัดลำดับความสำคัญของการดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort) เป็นต้น (๘) ศึกษาวิธีและลักษณะการโจมตี พร้อมทั้งระบุสาเหตุที่แท้จริงของภัยคุกคามทางไซเบอร์รวมถึงจุดอ่อนของระบบที่ถูกโจมตี (๙) ดำเนินการแจ้งไปยังผู้ที่รับผิดชอบในการเผชิญเหตุหรือผู้ที่เกี่ยวข้องผ่านช่องทางที่มีความปลอดภัย โดยคำนึงถึงระดับชั้นความลับและความสำคัญของข้อมูลเพื่อให้บุคคลดังกล่าวสามารถปฏิบัติหน้าที่ในการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น (๑๐) รายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างมีนัยสำคัญให้ผู้ที่เกี่ยวข้องทราบ ภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด (โดยหน่วยงานควบคุมหรือกากับดูแลอาจกำหนดให้นำข้อปฏิบัติตามแผนการกู้คืนของหน่วยงานมาประกอบการพิจารณาด้วยก็ได้) หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ๓ ของภาคผนวกแนบท้ายนี้ แล้วแต่กรณี
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	ให้หน่วยงานดำเนินการตามข้อ ๑ ถึงข้อ ๒ และดำเนินมาตรการเพิ่มเติม ดังนี้ (๑) จัดให้มีกลไกที่สามารถแจ้งเตือนได้ทันที (real-time alerts) เมื่อพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น (๒) จัดให้มีกลไกหรือระบบงานที่สามารถติดตามเหตุการณ์ และสามารถจัดเก็บและวิเคราะห์ข้อมูลต่าง ๆ เพื่อตรวจจับการเกิดภัยคุกคามทางไซเบอร์ได้โดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม) (๓) จัดให้มีการแจ้งเตือนเกี่ยวกับความผิดปกติของการใช้ทรัพยากรของระบบงาน เช่น แจ้งเตือนเมื่อหน่วยความจำที่ใช้ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เหลือน้อย (storage capacity warning) เมื่อมีการใช้หน่วยประมวลผลกลาง (CPU) หรือมีการใช้หน่วยความจำหลัก (RAM) ของอุปกรณ์เครือข่ายหรือระบบงานหลักที่สูงผิดปกติ หรือเมื่อมีการส่งข้อมูลออกนอกเครือข่ายมากผิดปกติ เป็นต้น (๔) วิเคราะห์ข้อมูลและค้นหาความสัมพันธ์ของข้อมูลกับเหตุการณ์ต่าง ๆ (information correlation) โดยอาจรับข้อมูลจากแหล่งข้อมูลอื่น ๆ นอกเหนือจากข้อมูลในระบบ เพื่อเพิ่มความสามารถในการรับรู้และดำเนินการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

ตารางที่ ๒.๓ การดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง	(๑) ดำเนินการตามแนวทางหรือวิธีการในการจำกัดขอบเขตและระงับภัยคุกคามทางไซเบอร์ โดยที่แนวทางหรือวิธีการดังกล่าวจะต้องมีหลักเกณฑ์ที่ชัดเจนเพื่อใช้ประกอบการตัดสินใจในการดำเนินการ ทั้งนี้ แนวทางดังกล่าวรวมถึง (๑.๑) การดำเนินการเชิงเทคนิค เช่น การลบมัลแวร์ การปิดการใช้งานบัญชีของผู้ใช้งานที่ถูกละเมิด การปิดระบบหรือตัดการเชื่อมต่อของระบบจากเครือข่ายภายหลังการเก็บหลักฐานหรือข้อมูลที่จำเป็นเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดีแล้ว เป็นต้น (๑.๒) การดำเนินการเชิงบริหาร เช่น กำหนดแนวทางดำเนินการหรือการตัดสินใจของฝ่ายบริหารของหน่วยงาน การสื่อสารทั้งภายในและภายนอกหน่วยงาน เป็นต้น (๑.๓) การเตรียมการเพื่อดำเนินการทางกฎหมายกับผู้กระทำความผิด (๒) ดำเนินการตามแนวปฏิบัติที่เกี่ยวข้องเพื่อเก็บรวบรวมและจัดการหลักฐานต่าง ๆ ที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์โดยทันทีหลังจากที่ตรวจพบ เช่น การจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้เมื่อปิดอุปกรณ์ (volatile data) การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อมูลเกี่ยวกับมัลแวร์ ข้อมูลสถานะของระบบ (system snapshot) หรือข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิค และเพื่อทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี (๓) ดำเนินการเพื่อให้มีการระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุหมายเลขประจำเครื่อง (IP address) การระบุช่องทางที่ผู้โจมตีใช้ การค้นหาและวิจัยที่มาของการโจมตีจากแหล่งข้อมูลต่าง ๆ เช่น ฐานข้อมูลภัยคุกคามทางไซเบอร์ที่รวบรวมข้อมูลจากหลายแหล่ง เป็นต้น (๔) ประสานงานเพื่อแจ้งหรือรายงานสถานการณ์การรับมือภัยคุกคามทางไซเบอร์และความคืบหน้าในการตอบสนองไปยังบุคคลหรือหน่วยงานที่เกี่ยวข้องตลอดจนผู้ที่อาจได้รับผลกระทบ อย่างทันท่วงที โดยอาจขอความช่วยเหลือไปยังบุคคลหรือหน่วยงานต่าง ๆ โดยเฉพาะการเกิดภัยคุกคามทางไซเบอร์ที่จัดอยู่ในหมวดหมู่ที่ ๑, ๒, ๔, ๕ และ ๗ ตามที่ระบุในข้อ ๑ ของภาคผนวกแนบท้ายนี้ ทั้งนี้ ในการแจ้งหรือรายงานสถานการณ์นั้น หน่วยงานควรเลือกใช้ช่องทางที่มีความเหมาะสมและปลอดภัยและดำเนินการแจ้งหรือรายงานเหตุภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ๓ ของภาคผนวกแนบท้ายนี้ แล้วแต่กรณี

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	(๕) ดำเนินการจัดการกับช่องโหว่ทั้งหมดที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ และดำเนินการตามวิธีการป้องกันระบบจากความเสียหายที่อาจเกิดขึ้นเพิ่มเติม เช่น การปรับเปลี่ยนการควบคุมการเข้าถึงเครือข่าย (อาทิ ไฟร์วอลล์) การติดตั้งลายเซ็นของ Anti-Virus หรือ IDS / IPS ใหม่ หรือการเปลี่ยนแปลงทางกายภาพในโครงสร้างพื้นฐาน และดำเนินการระงับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยทันทีหลังจากที่ตรวจพบ เป็นต้น (๖) ดำเนินการที่เกี่ยวข้องเพื่อให้มั่นใจว่าระบบงานต่าง ๆ ยังคงสามารถใช้งานได้ตามปกติภายในกรอบระยะเวลาที่กำหนด (restore within time period) เช่น การกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ (integrity restoration) การสร้างระบบงานขึ้นใหม่ (rebuild) การแทนที่ไฟล์ที่ได้รับผลกระทบ (replace) การติดตั้งโปรแกรมคอมพิวเตอร์ (install) การเปลี่ยนแปลงรหัสผ่าน และการรักษาความปลอดภัยทางเครือข่าย (securing network) เป็นต้น (๗) สร้างมาตรการป้องกันทั้งเชิงรุกและเชิงรับ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะคล้ายคลึงกันเกิดขึ้นอีกในอนาคต เช่น การเพิ่มมาตรการเฝ้าระวังสัญญาณเตือนและเหตุการณ์ต่าง ๆ ที่มีความเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นแล้ว เป็นต้น (๗) สร้างมาตรการป้องกันทั้งเชิงรุกและเชิงรับเพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะคล้ายคลึงกันเกิดขึ้นอีกในอนาคต เช่น การเพิ่มมาตรการเฝ้าระวังสัญญาณเตือนและเหตุการณ์ต่าง ๆ ที่มีความเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นแล้วเป็นต้น
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	ให้หน่วยงานดำเนินการตามข้อ ๑ และดำเนินมาตรการเพิ่มเติม ดังนี้ (๑) หากมีความจำเป็น ให้หน่วยงานดำเนินการใช้ระบบงานสำรองสำหรับการประมวลผล (alternate processing) การจัดเก็บข้อมูล (storage site) และกู้คืนข้อมูลที่เกี่ยวข้องกับการทำรายการหรือการดำเนินธุรกรรมต่าง ๆ (transaction recovery) (๒) ส่งคำแจ้งเตือนเพื่อขอรับการสนับสนุน ความช่วยเหลือ หรือประสานความร่วมมือไปยังหน่วยงานที่เกี่ยวข้อง (supply chain coordination) รวมถึงแจ้งไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (๓) ดำเนินการตามนโยบายการรายงานเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นภายในหน่วยงานซึ่งครอบคลุมถึงรูปแบบ ระดับความลับ และเนื้อหาที่ต้องรายงาน ลำดับชั้นการรายงาน กำหนดเวลา เครื่องมือที่ใช้รายงาน (โดยอาจพิจารณาใช้เครื่องมือที่สามารถช่วยรายงานภัยคุกคามโดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม))

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	(๔) ให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หน่วยงานควบคุมหรือกำกับดูแล พนักงานเจ้าหน้าที่ หรือบุคคลอื่นใดที่ปฏิบัติหน้าที่หรือได้รับมอบหมายให้ปฏิบัติหน้าที่ตามกฎหมาย (๕) พิจารณาจัดให้มีกลไกที่สามารถทางานได้โดยอัตโนมัติ ในการรับมือหรือสนับสนุนการรับมือเมื่อเกิดภัยคุกคามทางไซเบอร์ (automated incident handling processes) (ถ้าหน่วยงานมีความพร้อม)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	ให้หน่วยงานดำเนินการตามข้อ ๑ ถึงข้อ ๒ และดำเนินมาตรการเพิ่มเติม ดังนี้ (๑) ดำเนินการตามแผนการทำงานในการกู้คืนระบบงานต่าง ๆ เพื่อให้ระบบสามารถให้บริการได้ภายในกรอบระยะเวลาที่กำหนด (restore within time period) โดยอาศัยความรู้จากทีมผู้เชี่ยวชาญด้านต่าง ๆ เพื่อให้การกู้คืนระบบและเครือข่ายของหน่วยงานทำได้อย่างรวดเร็ว

หมายเหตุ: ในกรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้นแล้วแต่หน่วยงานยังไม่สามารถระบุระดับของภัยคุกคามทางไซเบอร์โดยใช้ปัจจัยที่ใช้ในการประเมินตามที่ระบุในตารางที่ ๑ ของเอกสารแนบ ๑ ได้ ซึ่งอาจเกิดจากการที่หน่วยงานยังไม่สามารถรวบรวมรายละเอียดหรือข้อมูลที่จำเป็นเพื่อใช้ในการวิเคราะห์ได้ในช่วงแรก หรือไม่ว่าด้วยเหตุอื่นใดก็ตาม ให้หน่วยงานดำเนินการประเมินผลกระทบเบื้องต้น โดยพิจารณาจากตัวอย่างตามที่ระบุในข้อ ๑ ของภาคผนวกแนบท้ายนี้ จนกว่าจะมีข้อมูลหรือปรากฏหลักฐานที่เพียงพอต่อการวิเคราะห์เพื่อระบุระดับของภัยคุกคามทางไซเบอร์

ตารางที่ ๒.๔ การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	ภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ ให้หน่วยงานพิจารณาดำเนินการดังนี้ (๑) นำเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและมีลักษณะเป็นภัยคุกคามทางไซเบอร์ที่มีนัยสำคัญมาเป็นกรณีศึกษา เช่น การพิจารณาถึงจุดอ่อนของโครงสร้างพื้นฐานของบริการ นโยบายและกระบวนการ การฝึกบุคลากร การระบุผู้มีอำนาจดำเนินงาน และเครื่องมือที่ใช้ เป็นต้น และหาแนวทางเพื่อเตรียมการรับมือและป้องกันการเกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะดังกล่าวร่วมกับบุคคลหรือหน่วยงานที่เกี่ยวข้อง (๒) รวบรวมข้อมูลการดำเนินงานที่เกี่ยวข้องกับการรับมือภัยคุกคามทางไซเบอร์ (โดยอาจดำเนินการเป็นรายสัปดาห์หรือรายเดือน) เช่น จำนวนของภัยคุกคามทางไซเบอร์ที่เกิดขึ้น เวลาที่ใช้ในการจัดการกับภัยคุกคามทางไซเบอร์ประเภทต่าง ๆ และวัตถุประสงค์ของการโจมตี เป็นต้น เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน (๓) ปรับปรุงมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับให้มีความเหมาะสม และเป็นปัจจุบัน (๔) เก็บรักษาข้อมูลและหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี ตามแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์ที่หน่วยงานได้กำหนด

อนึ่งแนวปฏิบัติพื้นฐาน (Security Control Baselines) ตามรายละเอียดที่กำหนด ไว้ในตารางที่ ๒.๑ – ตารางที่ ๒.๔ นี้ เป็นเพียงแนวทางที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเห็นว่ามีความเหมาะสมที่จะช่วยให้หน่วยงานสามารถดาเนินมาตรการเตรียมการและป้องกัน รับมือปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับได้อย่างมีประสิทธิภาพ และสามารถบรรลุวัตถุประสงค์ตามหลักการของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และที่แก้ไขเพิ่มเติม (ถ้ามี) ได้ อย่างไรก็ดี หน่วยงานสามารถหารือร่วมกับหน่วยงานควบคุมหรือกำกับดูแล เพื่อให้มีแนวทางการดำเนินมาตรการที่เหมาะสมและสอดคล้องกับลักษณะการดำเนินภารกิจ การให้บริการหรือทรัพยากรที่มีอยู่ภายใต้ความรับผิดชอบของหน่วยงานได้

๑๖

ภาคผนวก
ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม
และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

ข้อ ๑ การจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย
๐	เหตุการณ์จำลอง และ การฝึกจู่โจม ของหน่วยงานเอง (Training and Exercises)
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

ข้อ ๒ ตัวอย่างลักษณะภัยคุกคามทางไซเบอร์แยกตามระดับต่าง ๆ

	หมวดหมู่ภัยคุกคาม						
ประเภทอุปกรณ์เครือข่าย	๑	๒	๓	๔	๕	๖	๗
Backbone	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เราเตอร์	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายสาหรับการจัดการเครือข่าย หรือ ดูแลความปลอดภัย	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายที่ไม่ได้ให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	วิกฤต	ร้ายแรง	ร้ายแรง
เครื่องแม่ข่ายที่เปิดให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง
เครื่องเวิร์กสเตชัน	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง

[๔] การแจ้งหรือรายงานภัยคุกคามตามหมวดนี้เกิดขึ้นเมื่อผู้เผชิญเหตุยังไม่ทราบรายละเอียดภัยคุกคาม และ กำลังดำเนินการวิเคราะห์เหตุการณ์ (เช่น อาจอยู่ในช่วงแรก ๆ ที่พบการกระทำผิด) โดยหากทราบผลของการสอบสวนแล้ว ผู้รายงานควรเปลี่ยนเป็นหมวดอื่นให้ถูกต้อง และ ในรายงานสรุปปิดเหตุการณ์ ไม่ควรมีภัยคุกคามที่อยู่ในหมวดนี้ เนื่องจากการวิเคราะห์สอบสวนเสร็จสิ้นแล้ว)

ข้อ ๓ ตัวอย่างกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์

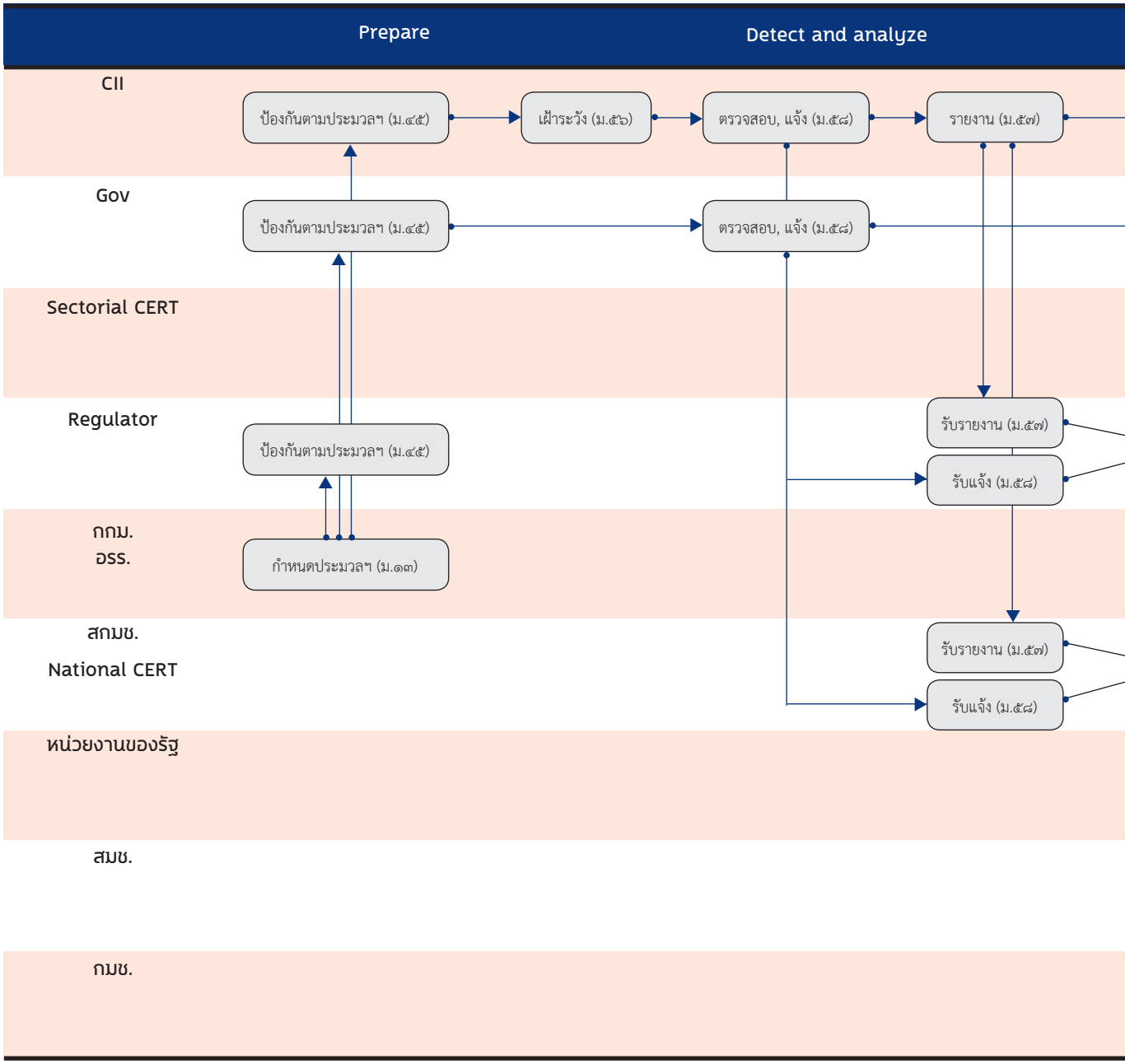
หมวดหมู่ภัยคุกคามทางไซเบอร์	ระดับภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้หน่วยงานควบคุมหรือกำกับดูแล (ภายในเวลา)	การส่งรายงานให้สำนักงาน (ภายในเวลา)
๑	ทุกเหตุการณ์	๓๐ นาที	๒ ชั่วโมง	๔ ชั่วโมง
๒	ทุกเหตุการณ์	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๓	ทุกเหตุการณ์	๓๐ นาที	๒ ชั่วโมง	๘ ชั่วโมง
๔	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๑ ชั่วโมง	๒ ชั่วโมง
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๕	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๑ ชั่วโมง	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๒ ชั่วโมง	๔ ชั่วโมง
๖	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๑ ชั่วโมง	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๒ ชั่วโมง	๔ ชั่วโมง
๗	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๑๐ นาที	๑ ชั่วโมง	๑ ชั่วโมง
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๘	-	๒๐ นาที	ตามเวลาที่ต้องใช้ในการสืบสวน	๔ ชั่วโมง
๙	-	-	๔ ชั่วโมง	๑๒ ชั่วโมง

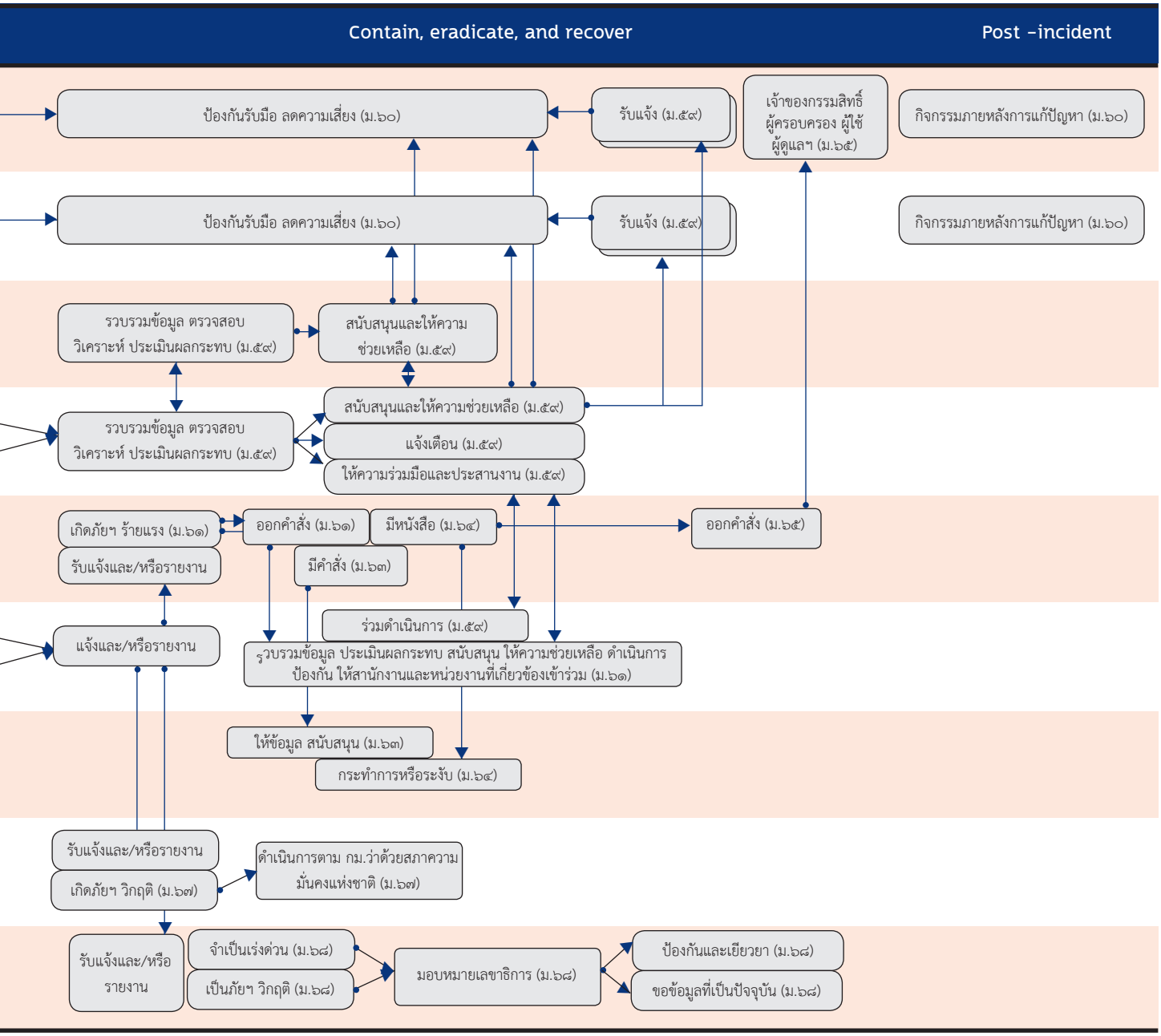
ผนวก ง

กระบวนการรับมือเหตุภัยคุกคามทางไซเบอร์

(DRAFT for National Cyber Exercise 2022 ONLY)

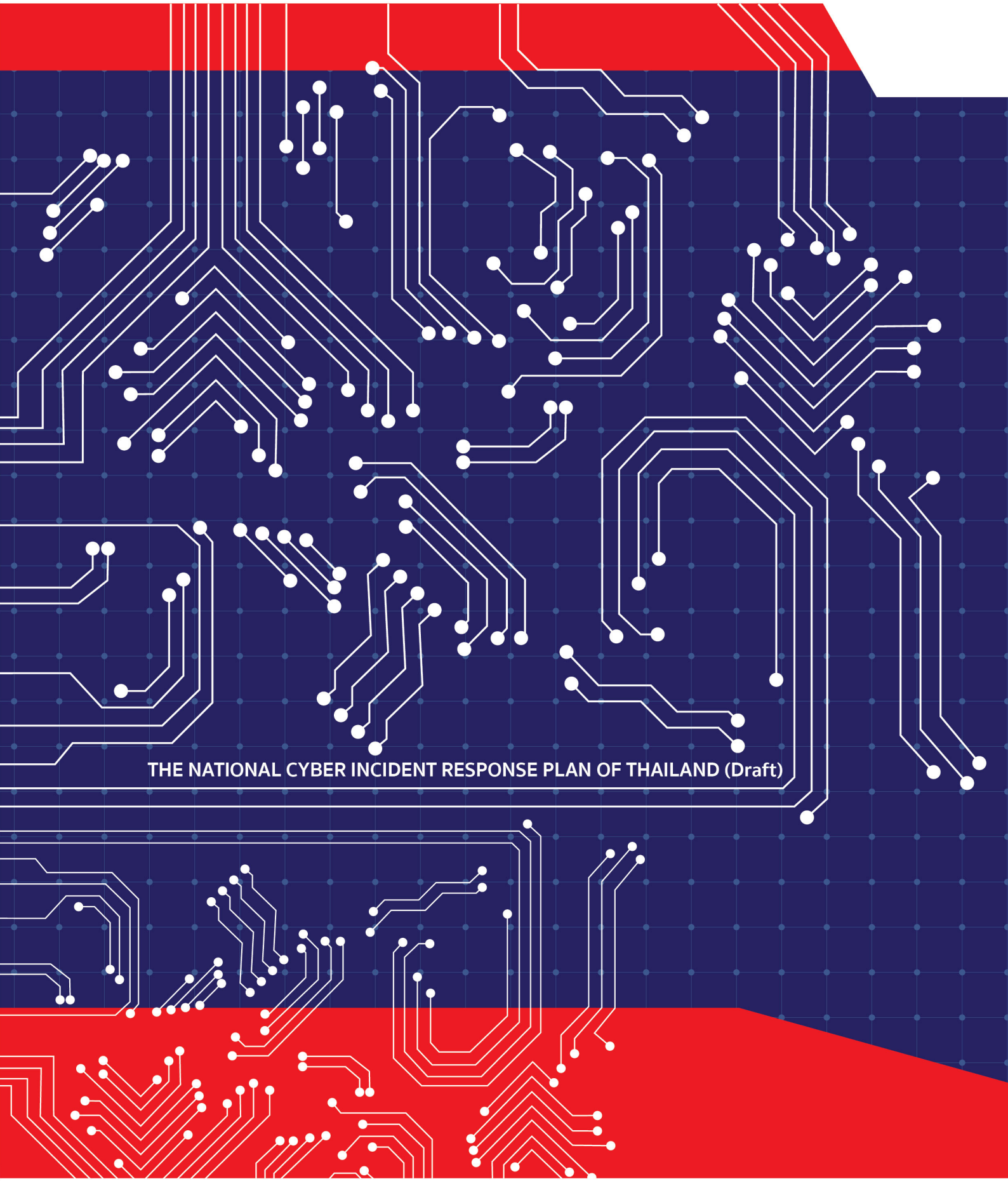
NATIONAL CYBER INCIDENT RESPONSE WORKFLOW




Contain, eradicate, and recover
Post -incident
ป้องกันรับมือ ลดความเสี่ยง (ม.๖๐)
รับแจ้ง (ม.๕๙)
เจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้ ผู้ดูแลฯ (ม.๖๕)
กิจกรรมภายหลังการแก้ปัญหา (ม.๖๐)
ป้องกันรับมือ ลดความเสี่ยง (ม.๖๐)
รับแจ้ง (ม.๕๙)
กิจกรรมภายหลังการแก้ปัญหา (ม.๖๐)
รวบรวมข้อมูล ตรวจสอบ วิเคราะห์ ประเมินผลกระทบ (ม.๕๙)
สนับสนุนและให้ความช่วยเหลือ (ม.๕๙)
สนับสนุนและให้ความช่วยเหลือ (ม.๕๙)
รวบรวมข้อมูล ตรวจสอบ วิเคราะห์ ประเมินผลกระทบ (ม.๕๙)
แจ้งเตือน (ม.๕๙)
ให้ความร่วมมือและประสานงาน (ม.๕๙)
เกิดภัยฯ ร้ายแรง (ม.๖๑)
รับแจ้งและ/หรือรายงาน
ออกคำสั่ง (ม.๖๑)
มีหนังสือ (ม.๖๔)
ออกคำสั่ง (ม.๖๕)
มีคำสั่ง (ม.๖๓)
ร่วมดำเนินการ (ม.๕๙)
แจ้งและ/หรือรายงาน
รวบรวมข้อมูล ประเมินผลกระทบ สนับสนุน ให้ความช่วยเหลือ ดำเนินการป้องกัน ให้สานักงานและหน่วยงานที่เกี่ยวข้องเข้าร่วม (ม.๖๑)
ให้ข้อมูล สนับสนุน (ม.๖๓)
กระทำการหรือระงับ (ม.๖๔)
รับแจ้งและ/หรือรายงาน
เกิดภัยฯ วิกฤติ (ม.๖๗)
ดำเนินการตาม กม.ว่าด้วยสภาความมั่นคงแห่งชาติ (ม.๖๗)
รับแจ้งและ/หรือรายงาน
จำเป็นเร่งด่วน (ม.๖๘)
เป็นภัยฯ วิกฤติ (ม.๖๘)
มอบหมายเลขาธิการ (ม.๖๘)
ป้องกันและเยียวยา (ม.๖๘)
ขอข้อมูลที่เป็นปัจจุบัน (ม.๖๘)

ผนวก จ

ชุดที่	รายการแจกจ่าย
๑ - ๑๙	หน่วยงานควบคุมหรือกำกับดูแล
๒๐ - ๗๐	หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๗๑ – ๗๒	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectorial CERT)
๗๓ – ๘๓	หน่วยงานอื่น ๆ ที่เกี่ยวข้อง
๘๔ – ๒๐๐	สำรองไว้แจกจ่ายหน่วยงานอื่น ๆ ที่เกี่ยวข้อง
๒๐๑ - ๓๐๐	สำรองไว้แจกจ่าย สกมช.



NCSA
สกมช
สำนักงานคณะกรรมการการรักษา
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ