ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. ๒๕๖๔

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้มีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติขึ้นเป็นหน่วยงานภายในสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

อาศัยอำนาจตามความในมาตรา ๒๒ วรรคสอง แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ ๑/๒๕๖๔ เมื่อวันที่ ๒๕ มิถุนายน ๒๕๖๔ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศฉบับนี้ เพื่อกำหนดหน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. ๒๕๖๔”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“คณะกรรมการ” หมายความว่า คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“หน่วยงานภายใต้การดูแล” หมายความว่า หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานที่ทำหน้าที่เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานเอกชนอื่นตามที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติได้รับมอบหมายจากคณะกรรมการให้ดำเนินการ

ข้อ ๔ ในการดำเนินการใด ๆ ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ รวมถึงการติดต่อ ประสานงาน หรือการแจ้งเตือนที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติจัดให้มีหลักเกณฑ์ เงื่อนไข และวิธีการในการจัดชั้นความลับของข้อมูลต่าง ๆ การกำหนดสิทธิในการเข้าถึงข้อมูลและการดำเนินการอื่นใดที่เกี่ยวข้อง เพื่อรักษาความลับ (confidentiality) ความถูกต้อง (integrity) ตลอดจนความพร้อมในการใช้งาน (availability) ของข้อมูลที่เกี่ยวข้อง

ข้อ ๕ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติมีหน้าที่และอำนาจ รวมทั้งให้มีการดำเนินมาตรการในด้านต่าง ๆ ดังต่อไปนี้

๕.๑ การดำเนินมาตรการเชิงรุกเพื่อป้องกันและเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ให้เป็นไปตามหลักเกณฑ์ ดังนี้

๕.๑.๑ ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานภายใต้การดูแล เพื่อเฝ้าระวัง ติดตาม และเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

๕.๑.๒ เป็นศูนย์กลางเครือข่ายข้อมูลและส่งเสริมความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยอาจประสานงานหรือร่วมมือกับเครือข่ายหรือภาคีทั้งในและต่างประเทศ เพื่อรับ ส่งต่อ หรือแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์และเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

๕.๑.๓ จัดทำข้อมูลทางสถิติด้านการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ ตลอดจนข้อมูลการแจ้งเตือนที่สำคัญ และข้อมูลอื่น ๆ ที่เกี่ยวข้องเพื่อเผยแพร่ต่อสาธารณะ

๕.๑.๔ วิเคราะห์และตรวจสอบข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น ดำเนินการเพื่อป้องกันปัญหาที่อาจเกิดขึ้น รวมถึงการเผยแพร่ข้อมูลที่มีความจำเป็นเพื่อให้หน่วยงานภายใต้การดูแลสามารถดำเนินมาตรการป้องกันหรือจัดการกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น เช่น การให้คำแนะนำแก่หน่วยงานดังกล่าวในการตรวจจับการบุกรุก และการวิเคราะห์ข้อมูล เป็นต้น

๕.๑.๕ ให้การแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น หรือให้คำเตือนเกี่ยวกับช่องโหว่ที่อาจถูกใช้เป็นช่องทางในการก่อภัยคุกคามทางไซเบอร์ เพื่อให้หน่วยงานภายใต้การดูแลดำเนินการเพื่อให้มีการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือระบบงานที่มีความสำคัญอื่น ๆ ได้อย่างทันท่วงที

๕.๑.๖ ติดตามความก้าวหน้าด้านเทคโนโลยีต่าง ๆ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับการป้องกันภัยคุกคามทางไซเบอร์หรือแนวปฏิบัติพื้นฐาน (baseline) ในการป้องกันหรือเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

๕.๑.๗ เมื่อได้รับการร้องขอจากหน่วยงานภายใต้การดูแล หรือเมื่อได้รับการประสานงานในกรณีที่คาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้นกับหน่วยงานดังกล่าว ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติอาจพิจารณาดำเนินการ ดังนี้

(๑) รวบรวมข้อมูล ติดตาม วิเคราะห์ และประมวลผลข้อมูลเพื่อทำวิจัยเชิงรุกเกี่ยวกับรูปแบบของการเกิดภัยคุกคามทางไซเบอร์ เพื่อประเมินผลกระทบและแนวโน้มของการเกิดภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ

(๒) ให้การช่วยเหลือ แนะนำ และสนับสนุนในการดำเนินมาตรการป้องกันตามแนวทางปฏิบัติที่ดี (best practice) เพื่อเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

(๓) ประเมินความเสี่ยงและช่องโหว่ที่อาจถูกใช้ในการก่อภัยคุกคามทางไซเบอร์เพื่อนำไปสู่การจัดการช่องโหว่ การดำเนินมาตรการป้องกัน หรือกระทำการอื่นใดเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

(๔) ตรวจจับเหตุการณ์ที่อาจนำมาสู่การบุกรุก วิเคราะห์สิ่งบอกเหตุการณ์ หรือดำเนินการอื่นใดที่เกี่ยวข้องเพื่อตรวจสอบโปรแกรม หรือค้นหาสิ่งที่ไม่พึงประสงค์ (malicious code) ซึ่งอาจเป็นอันตรายต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือระบบงานที่มีความสำคัญอื่น ๆ

ทั้งนี้ เพื่อประโยชน์ในการประสานงานและการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติดำเนินการเพื่อให้มีการรับลงทะเบียนข้อมูลและจัดทำบัญชีช่องทางการติดต่อ (point of contact) ของหน่วยงานภายใต้การดูแล เพื่อใช้เป็นช่องทางหลักในการติดต่อสื่อสารระหว่างศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติกับหน่วยงานดังกล่าว

๕.๒ การดำเนินมาตรการเชิงรับเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้เป็นไปตามหลักเกณฑ์ ดังนี้

๕.๒.๑ เป็นศูนย์กลางในการรับและแจ้งเหตุเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นทั้งในประเทศและต่างประเทศ และประสานงานกับหน่วยงานภายใต้การดูแล เพื่อตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์อย่างเหมาะสมและทันท่วงที ตลอดจนให้การสนับสนุนข้อมูลต่าง ๆ ที่จำเป็นแก่หน่วยงานดังกล่าว เพื่อดำเนินการแก้ไขเหตุภัยคุกคามทางไซเบอร์ โดยจัดให้มีช่องทางในการรับและแจ้งเหตุผ่านระบบอิเล็กทรอนิกส์ที่กำหนดขึ้นโดยเฉพาะหรือช่องทางอื่นใดตามที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติกำหนด

๕.๒.๒ พิจารณาความเหมาะสมในการกำหนดระดับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นตามที่ได้รับแจ้งจากหน่วยงานภายใต้การดูแล โดยอาจพิจารณากำหนดความเร่งด่วนตามที่ได้รับแจ้งหรือกำหนดความเร่งด่วนขึ้นใหม่จากลักษณะหรือผลกระทบจากภัยคุกคามทางไซเบอร์ และให้คำแนะนำในการกำหนดแผนการรับมือและแก้ไขภัยคุกคามทางไซเบอร์ที่เหมาะสมเพื่อจำกัดขอบเขตความเสียหาย

๕.๒.๓ ติดตามการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ ผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ และผลการตอบสนองและรับมือเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

๕.๒.๔ เมื่อได้รับการร้องขอจากหน่วยงานภายใต้การดูแล หรือเมื่อได้รับการประสานงานในกรณีที่คาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้นกับหน่วยงานดังกล่าว ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติอาจพิจารณาดำเนินการ ดังนี้

(๑) ให้การช่วยเหลือ แนะนำ และสนับสนุนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น เช่น การช่วยวิเคราะห์ต้นเหตุของภัยคุกคาม โปรไฟล์ของผู้โจมตี วิธีการระงับเหตุการณ์ตอบโต้ผู้บุกรุกและการกำจัดช่องโหว่ โดยอาจเข้าไปในสถานที่ที่เกิดเหตุการณ์ หรือดำเนินการผ่านวิธีการทางอิเล็กทรอนิกส์ที่ใช้ในการติดต่อสื่อสารจากสถานที่ปฏิบัติงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

(๒) ให้การช่วยเหลือ แนะนำ และสนับสนุนในการฟื้นฟูเพื่อให้สามารถกลับมาดำเนินภารกิจหรือให้บริการได้ต่อไปภายหลังการระงับเหตุภัยคุกคามทางไซเบอร์เสร็จสิ้น

(๓) ให้การช่วยเหลือ แนะนำ และสนับสนุนในการดำเนินกระบวนการทางนิติวิทยาศาสตร์ การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล การเชื่อมโยงข้อมูลภัยคุกคามทางไซเบอร์จากแหล่งข้อมูลต่าง ๆ ตลอดจนการสืบสวนหรือสอบสวนเกี่ยวกับการกระทำความผิดที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์

๕.๒.๕ จัดทำรายงานข้อมูลผลการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นทั้งในกรณีที่ได้รับทราบจากการแจ้งเหตุของผู้เกี่ยวข้อง รวมถึงกรณีที่พบเห็นเหตุการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อรายงานต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ทั้งนี้ เพื่อประโยชน์ในการรับมือกับเหตุภัยคุกคามทางไซเบอร์ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติอาจดำเนินการรวบรวมข้อมูลการโจมตีทางไซเบอร์ที่เกิดขึ้น เพื่อใช้เป็นข้อมูลในการศึกษา วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อนำไปสู่การดำเนินมาตรการเชิงรุกในการป้องกันและเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ในอนาคต

๕.๓ การดำเนินมาตรการด้านการบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้เป็นไปตามหลักเกณฑ์ ดังนี้

๕.๓.๑ ผลักดันและสนับสนุนให้เกิดการสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อนำไปสู่การดำเนินมาตรการในการป้องกันและการรักษาความมั่นคงปลอดภัยไซเบอร์

๕.๓.๒ ยกระดับความรู้ความสามารถของหน่วยงานภายใต้การดูแลเพื่อเตรียมความพร้อมในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และสามารถยกระดับการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบงานที่มีความสำคัญอื่น ๆ

๕.๓.๓ เมื่อได้รับการร้องขอจากหน่วยงานภายใต้การดูแล ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติอาจพิจารณาดำเนินการ ดังนี้

(๑) ให้การช่วยเหลือ แนะนำ และสนับสนุนในการประเมินความเสี่ยงของการเกิดภัยคุกคามทางไซเบอร์ โดยใช้กระบวนการเรียนรู้ที่ได้รับจากการดำเนินมาตรการเชิงรุกเพื่อป้องกันและเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ และการดำเนินมาตรการเชิงรับเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น เพื่อช่วยให้หน่วยงานดังกล่าวสามารถวางแผนการรับมือในกรณีที่ต้องเผชิญเหตุภัยคุกคามทางไซเบอร์

(๒) ให้การช่วยเหลือ แนะนำและสนับสนุนในการจัดทำแผนความต่อเนื่องของการดำเนินงาน (business continuity plan) เพื่อรับมือในกรณีที่เกิดเหตุภัยคุกคามทางไซเบอร์ แผนการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (critical information infrastructure protection plan) และแผนฟื้นฟู (disaster recovery plan) ภายหลังเกิดภัยคุกคามทางไซเบอร์

๕.๓.๔ เพื่อให้การบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการได้อย่างมีประสิทธิภาพและมีประสิทธิผล ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติดำเนินการ ดังนี้

(๑) ระบุตัวชี้วัดและติดตามผลการดำเนินงาน เพื่อประเมินคุณภาพของการดำเนินการ เช่น ระยะเวลาที่ใช้ตอบสนองต่อการร้องขอ ระยะเวลาที่ใช้ต่อการดำเนินงานในสถานการณ์ต่าง ๆ และจำนวนรายงานหรือคู่มือที่เกี่ยวข้องกับพันธกิจ เป็นต้น

(๒) กำหนดแนวทางการดำเนินงานด้านนโยบายและการปฏิบัติเป็นระดับ (phase) โดยอาจใช้โมเดลการวัดระดับขีดความสามารถขององค์กร (Capability Maturity Model หรือ “CMM”) เป็นเครื่องมือในการกำหนด

(๓) จัดให้มีระบบบริหารจัดการคุณภาพ (service management quality system) เพื่อติดตามผลการดำเนินงานและปรับปรุงการดำเนินงานอย่างต่อเนื่อง เพื่อให้เป็นไปตามผลการดำเนินงานที่ตั้งเป้าหมาย

(๔) กำหนดกระบวนการและขั้นตอน รวมถึงเครื่องมือที่จำเป็นเพื่อใช้สนับสนุนการให้บริการแก่หน่วยงานภายใต้การดูแล เช่น ระบบบันทึกภัยคุกคามและการติดตามการดำเนินงาน (ticketing system) และระบบบริหารจัดการงานต่าง ๆ (workflow management system) เป็นต้น

๕.๓.๕ ดำเนินกิจกรรมร่วมกับหน่วยงานของรัฐ หน่วยงานเอกชน องค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศ อันเป็นประโยชน์ต่อการบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และการรับมือกับภัยคุกคามทางไซเบอร์ตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมอบหมายเพิ่มเติม

ข้อ ๖ เพื่อประโยชน์ในการเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติให้การช่วยเหลือสนับสนุน หรือปฏิบัติงานร่วมกับพนักงานเจ้าหน้าที่ หรือสนับสนุนการดำเนินการของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในกิจการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์และการรับมือกับภัยคุกคามทางไซเบอร์ หรือปฏิบัติหน้าที่อื่นใดเพิ่มเติมได้ตามที่คณะกรรมการกำหนด

ประกาศ ณ วันที่ ๑๑ สิงหาคม พ.ศ. ๒๕๖๔
พลเอก ประวิตร วงษ์สุวรรณ
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ