สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐ อีเมล saraban@ncsa.or.th

ด่วนที่สุด

ที่ สกมช ๐๘๑๐/๔๕๗

๕ มิถุนายน ๒๕๖๘

เรื่อง ขอให้หน่วยงานดำเนินการตามแนวปฏิบัติขั้นพื้นฐานสำหรับการป้องกัน เฝ้าระวัง และรับมือภัยคุกคามทางไซเบอร์

เรียน หัวหน้าส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน องค์กรอิสระ หน่วยงานภาคเอกชน และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

อ้างถึง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

สิ่งที่ส่งมาด้วย ๑. แนวทางการตอบสนอง ป้องกัน เฝ้าระวัง และรับมือภัยคุกคามทางไซเบอร์

๒. แบบตอบรับการดำเนินการตามแนวทางการตอบสนอง ป้องกัน เฝ้าระวัง และรับมือภัยคุกคามทางไซเบอร์

ตามอ้างถึง ๑ มาตรา ๔๕ และ มาตรา ๒๒ (๖) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มีหน้าที่และอำนาจ “เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตามวิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์” ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ปัจจุบันสถาณการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานต่าง ๆ ภายในประเทศเพิ่มสูงขึ้นอย่างมีนัยสำคัญ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) หรือ ThaiCERT ได้ดำเนินการเฝ้าระวัง ตรวจสอบ และได้ร่วมเผชิญเหตุตอบสนองรับมือกับภัยคุกคามที่เกิดขึ้นหลายเหตุการณ์ พบว่ามีการโจมตีหน่วยงานและอาจส่งผลกระทบต่อการให้บริการประชาชน ดังนี้

๑. การโจมตีแบบ DDoS ต่อหน่วยงานในประเทศไทยหลายแห่ง ส่งผลให้บริการหยุดชะงักชั่วคราว

๒. การโจมตีทางไซเบอร์ต่อหน่วยงานของรัฐโดยใช้บัญชีผู้ใช้งาน (Credential) ที่เคยรั่วไหลในการเข้าสู่ระบบ โดยผู้โจมตีได้รับข้อมูลบัญชีผู้ใช้งาน (Credential) สำหรับการยืนยันตัวตนจากแหล่งซื้อขาย เช่น Dark Web หรือ Breach Forum รวมถึงมีการแชร์ข้อมูลบัญชีผู้ใช้งาน (Credential) ที่ขโมยมาได้ในแพลตฟอร์มการสื่อสารผ่านระบบอิเล็กทรอนิกส์ต่าง ๆ โดยผู้โจมตีจะใช้ข้อมูลที่ได้มาในการเข้าถึงช่องทางเครือข่ายภายในของหน่วยงาน อย่างเช่น ระบบ VPN และใช้ข้อมูลเหล่านั้นเข้าสู่ระบบงานสำคัญต่าง ๆ จากนั้นก็ทำการขโมยข้อมูลของหน่วยงานออกไปและโจมตีเพื่อทำลายระบบต่าง ๆ ด้วย Ransomware เป็นต้น

๓. การโจมตีในรูปแบบเปลี่ยนแปลงหน้าเว็บ (Web Defacement) เพื่อสร้างความไม่น่าเชื่อถือให้แก่หน่วยงาน

๔. Data Breach เหตุการณ์ที่ข้อมูลสำคัญขององค์กร เช่น ข้อมูลลูกค้า ข้อมูลส่วนบุคคล หรือข้อมูลทางธุรกิจ ถูกเข้าถึง ดัดแปลง หรือเปิดเผยโดยไม่ได้รับอนุญาต ซึ่งอาจเกิดจากการถูกแฮก การตั้งค่าระบบผิดพลาด หรือความประมาทของบุคลากร โดยเหตุการณ์นี้สามารถส่งผลกระทบรุนแรงต่อชื่อเสียง ความเชื่อมั่น และความเสียหายทางการเงินขององค์กร

/ในการนี้...

ในการนี้ เพื่อให้สามารถป้องกัน รับมือ และลดความซึ่งอาจส่งผลให้เกิดความเสียหายต่อระบบอย่างร้ายแรง และถูกขโมยข้อมูลสำคัญรวมถึงข้อมูลส่วนบุคคลของหน่วยงานและประชาชน สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จึงได้จัดทำแนวปฏิบัติขั้นพื้นฐานสำหรับตอบสนอง ป้องกันและรับมือสำหรับหน่วยงานระยะเร่งด่วน เพื่อมิให้สร้างผลกระทบต่อระบบสารสนเทศหรือประชาชนที่มาใช้บริการหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จึงขอให้หน่วยงานของท่านนำไปดำเนินการให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น และเมื่อได้รับหนังสือฉบับนี้ ขอความอนุเคราะห์ยืนยันการรับทราบหนังสือให้ สกมช. ทางอีเมล thaicert@ncsa.or.th ทันที และขอให้ผู้บริหารหน่วยลงนามยืนยันแจ้งผลการดำเนินการตามแบบตอบรับ (สิ่งที่ส่งมาด้วย) ให้ สกมช. ทราบทางอีเมล thaicert@ncsa.or.th อีกครั้ง ภายในวันที่ ๓๐ มิถุนายน ๒๕๖๘ ทั้งนี้ สกมช. จะได้รวบรวมรายงานผลให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) โดยมี นายกรัฐมนตรี เป็นประธาน เพื่อรับทราบต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป

ขอแสดงความนับถือ

พลอากาศตรี

(อมร ชมเชย)
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
โทรศัพท์ ๐ ๒๑๔๒ ๖๘๘๕ อีเมล thaicert@ncsa.or.th

พ.จ.อ.
(ภูริรพี หวีกสิกรรม)
ปลัดเทศบาล ปฏิบัติหน้าที่
นายกเทศมนตรีตำบลเวียงพางคำ