E. สคค. 231/2565

8303

บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ส่วนระบบคอมพิวเตอร์และเครือข่าย โทร. ๒๔๖๘

ที่ ศทส. ๔๔๑๙ /๒๕๖๕ **วันที่** ๗ พฤศจิกายน ๒๕๖๕

เรื่อง แจ้งเตือนการโจมตีต่อเว็บไซต์ของหน่วยงานภายใต้สังกัดของกรมชลประทาน สผค 9053 / 7 พ.ย.65

เรียน ผู้อำนวยการสำนัก กอง กลุ่ม ศูนย์ สถาบันและ ผส.ชป. ๑-๑๗

ด้วยกรมชลประทาน ได้รับแจ้งจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ว่าตรวจพบการโจมตีต่อเว็บไซต์ของหน่วยงานภายใต้สังกัดของกรมชลประทาน นั้น

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จึงขอแจ้งให้หน่วยงาน กำชับเจ้าหน้าที่ผู้รับผิดชอบดูแลเว็บไซต์ของหน่วยงาน ตรวจสอบ ติดตาม เฝ้าระวัง ป้องกัน เว็บไซต์ในความรับผิดชอบและปฏิบัติตามมาตรฐานรักษาความปลอดภัยสำหรับเว็บไซต์อย่างเคร่งครัด ป้องกันการนำไปใช้หลอกลวงอันจะส่งผลให้เกิดความเสียหาย แก่หน่วยงานของกรมชลประทาน ทั้งนี้ได้แนบคำแนะนำเบื้องต้นในการดูแลและป้องกันเว็บไซต์ของหน่วยงานเพื่อลดความเสี่ยงการถูกโจมตีเว็บไซต์ สำหรับผู้ดูแลระบบ มาด้วยแล้ว รายละเอียดตามเอกสารที่แนบ

จึงเรียนมาเพื่อโปรดพิจารณา

(นายนรเศรษฐ สองทอง)
ผอ.ทส.

เรียน ผอ.ส่วน ผอว.ภาค
เพื่อทราบดำเนินการ

(นายธเนศร์ สมบูรณ์)
ผส.บอ.

คำแนะนำเบื้องต้นในการดูแลและป้องกันเว็บไซต์ของหน่วยงานเพื่อลดความเสี่ยงถูกโจมตีเว็บไซต์

สำหรับผู้ดูแลระบบ

ด้วยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) แจ้งเตือนการโจมตีต่อเว็บไซต์ในหน่วยงานภายใต้กรมชลประทาน เพื่อป้องกันการนำไปใช้หลอกลวงอันจะส่งผลให้เกิดความเสียหายแก่หน่วยงาน อันจะก่อให้เกิดการกระทำผิดกฎหมาย ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และ พ.ร.บ. ความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ.๒๕๖๒ ได้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้รวบรวมวิธีการตรวจสอบ ติดตาม เฝ้าระวัง ป้องกัน เว็บไซต์เบื้องต้น ดังนี้

๑. ตรวจสอบและยืนยันสิทธิการเข้าระบบที่สำคัญของบัญชีผู้ใช้ให้สอดคล้องกับความจำเป็นเข้าถึงระบบและข้อมูล [๑]

๒. กำหนดรหัสผ่านการเข้าระบบที่ยากต่อการคาดเดา ควรมีความยาวไม่น้อยกว่า ๘ ตัวอักษร และใช้อักขระพิเศษ ไม่ตรงกับความหมายในพจนานุกรม เพื่อให้เดายากมากขึ้น [๑]

๓. หมั่นตรวจสอบและอัพเดตระบบปฏิบัติการที่ใช้ หรือซอฟแวร์ที่ใช้ ให้เป็นเวอร์ชั่นปัจจุบัน [๑]

๔. เพิ่มความระมัดระวังการเข้าใช้งานเว็บไซต์ที่ไม่เหมาะสม หรือไม่คลิกลิงค์หรือไฟล์แนบจากแหล่งที่มาไม่ชัดเจน หรือไม่รู้จัก ทั้งนี้เพื่อป้องกันการติดมัลแวร์ [๑]

๕. หากพบพิรุธว่าระบบถูกโจมตี เช่น ไม่สามารถเข้าใช้งานระบบ/เว็บไซต์ได้ หรือมีความล่าช้ากว่าปกติ ควรตรวจสอบข้อมูลการเข้าถึงระบบที่สำคัญ เช่น ข้อมูล Log ย้อนหลัง ๓๐ วัน เพื่อตรวจหาความผิดปกติในการเข้าถึงข้อมูล [๑]

๖. สำรองข้อมูลอย่างน้อย ๓ ชุด ทั้งแบบออฟไลน์และสำเนาข้อมูลในอุปกรณ์จัดเก็บ โดยไม่ให้เข้าถึงได้จากระบบงานปกติ [๑]

๗. พัฒนาระบบหรือจัดทำเว็บไซต์ให้ปลอดภัย โดยสามารถศึกษาข้อมูลเพิ่มเติมจากองค์กร OWASP ซึ่งเป็นองค์กรไม่แสวงหาผลกำไร โดยการใช้เทคโนโลยีการรักษาความมั่นคงปลอดภัยของเว็บไซต์ ได้ที่ https://owasp.org/ [๑]

<u>ตาม พ.ร.บ.การการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒</u> มาตรา ๕๘ [๒] ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว

อ้างอิง

๑. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

๒. สำนักเลขาธิการคณะรัฐมนตรี http://www.ratchakitcha.soc.go.th/DATA/PDF/๒๕๖๒/A/๐๖๙/T_๐๐๒๐.PDF