ที่ ศธ ๐๗๐๔๕.๐๗/๒๑๔

ศูนย์ส่งเสริมการเรียนรู้ระดับอำเภอเกาะช้าง
๒๒๒ หมู่ ๑ ต.เกาะช้าง อ.เกาะช้าง
จ.ตราด ๒๓๑๗๐

๒๙ พฤษภาคม ๒๕๖๙

เรื่อง แนวทางการป้องกันและคำแนะนำการรับมือภัยคุกคามจากโมเดลปัญญาประดิษฐ์ (AI)

เรียน ผู้อำนวยการสำนักงานส่งเสริมการเรียนรู้ประจำจังหวัดตราด

อ้างถึง หนังสือ สำนักงาน สกร.ประจำจังหวัดตราด ที่ ศธ ๐๗๐๔๕ /ว๘๙๒ ลงวันที่ ๑๙ พฤษภาคม ๒๕๖๙

สิ่งที่ส่งมาด้วย แบบตอบรับการตรวจสอบแนวทางการรับมือฯ จำนวน ๑ ฉบับ

ตามหนังสือที่อ้างถึง สำนักงานส่งเสริมการเรียนรู้ประจำจังหวัดตราด แจ้งให้ศูนย์ส่งเสริมการเรียนรู้ระดับอำเภอเกาะช้าง ดำเนินการรับทราบและนำแนวทางการป้องกันและคำปนะนำการับมือภัยคุกคามจากโมเดลปัญญาประดิษฐ์ (AI) ที่เกี่ยวข้องโดยเร่งด่วนตามความละเอียดแจ้งแล้วนั้น

ศูนย์ส่งเสริมการเรียนรู้ระดับอำเภอเกาะช้าง ได้ดำเนินการเรียบร้อยแล้ว ตามเอกสารที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ

(นายชยธร วัชรพงศ์ศิริ)
ผู้อำนวยการ สกร.ระดับอำเภอเกาะช้าง

กลุ่มอำนวยการ
งานบุคลากร
โทรศัพท์ ๐ ๓๙๕๑๐๘๐๕

แผนให้ตอบสนองเหตุกาณณ์ Incident Response Plan ให้ครอบคลุมสถานการณ์การโจมตีโดยใช้ AI เป็นเครื่องมือ
และกำหนดผู้รับผิดชอบแต่ละขั้นตอน

ขั้นตอน	แนวทางในการดำเนินงาน	ผู้รับผิดชอบ
๑. การป้องกัน (Prevention)	- กำหนดนโยบายการใช้ AI อย่างปลอดภัย - อบรมบุคลากรเรื่องภัยคุกคามจาก AI และ Cybersecurity - ติดตั้งโปรแกรมป้องกันไวรัสและระบบ Firewall - สำรองข้อมูลสำคัญเป็นประจำ	ผู้อำนวยการศูนย์ส่งเสริมการเรียนรู้ระดับอำเภอเกาะช้าง / ครูผู้ดูแลระบบ / เจ้าหน้าที่เทคโนโลยีอำเภอเกาะช้าง
๒. การเระวัง (Detection)	- ตรวจสอบอีเมล/ข้อความต้องสงสัยจาก AI Phishing - เฝ้าระวังการเข้าถึงข้อมูลผิดปกติ - ตรวจสอบการเผยแพร่ข้อมูลปลอมของหน่วยงาน	เจ้าหน้าที่ / เจ้าหน้าที่เทคโนโลยีอำเภอเกาะช้าง / บุคลากรทุกคน
๓. การตอบสนองเหตุการณ์ (Response)	- แยกอุปกรณ์ที่ถูกโจมตีออกจากเครือข่ายทันที - แจ้งผู้บริหารและผู้เกี่ยวข้อง - เก็บหลักฐานการโจมตี เช่น ภาพหน้าจอ อีเมล ลิงก์	ครูผู้ดูแลระบบ / เจ้าหน้าที่เทคโนโลยีอำเภอเกาะช้าง / คณะทำงานความปลอดภัยข้อมูล
๔. การแก้ไขและฟื้นฟู (Recovery)	- กู้คืนข้อมูลจากระบบสำรอง - เปลี่ยนรหัสผ่านและตรวจสอบสิทธิ์การเข้าถึง - ตรวจสอบความปลอดภัยก่อนเปิดใช้งานระบบอีกครั้ง	เจ้าหน้าที่ / เจ้าหน้าที่เทคโนโลยีอำเภอเกาะช้าง / ผู้บริหารสถานศึกษา
๕. การสรุปและป้องกันซ้ำ (Lessons Learned)	- ประชุมสรุปเหตุการณ์และผลกระทบ - ปรับปรุงมาตรการรักษาความปลอดภัย - จัดทำรายงานและแนวทางการป้องกันเพิ่มเติม	ผู้อำนวยการศูนย์ส่งเสริมการเรียนรู้ระดับอำเภอเกาะช้าง / คณะกรรมการ / เจ้าหน้าที่เทคโนโลยีอำเภอเกาะช้าง

ลงชื่อ.....
นางสาววาสนา อุ้ยอลงกรณ์
เจ้าหน้าที่แผน

ลงชื่อ.....
นายชยธร วัชรพงศ์ศิริ
ผู้อำนวยการ สกร.ระดับอำเภอเกาะช้าง

แบบตอบรับการตรวจสอบแนวทางการรับมือกรณี AI ถูกใช้เป็นเครื่องมือโจมตีทางไซเบอร์

(ตามหนังสือ สกมช. TLP:CLEAR)

หน่วยงาน: ศูนย์ส่งเสริมการเรียนรู้ [illegible] วันที่: ๒๙ / พ.ค. / ๒๕๖๙

แบบตอบรับการตรวจสอบแนวทางการรับมือกรณี AI ถูกใช้เป็นเครื่องมือโจมตีทางไซเบอร์			
ลำดับ	**หัวข้อและแนวทางปฏิบัติ**	**รายละเอียดดำเนินการ**	**ดำเนินการเรียบร้อย**
1. มาตรการเร่งด่วน			
1	**มาตรการเร่งด่วน**	ตรวจสอบและแก้ไขช่องโหว่ โดยเฉพาะระบบที่เปิดให้บริการจากภายนอก เพื่อลดความเสี่ยงจากการถูกค้นหาและโจมตีโดยอัตโนมัติ	☐
		บังคับใช้การพิสูจน์ตัวตนหลายปัจจัย (MFA) สำหรับบัญชีผู้ดูแลระบบ ระบบบริหารจัดการ อุปกรณ์สำคัญ และบริการคลาวด์ที่เกี่ยวข้อง ในกรณีที่ไม่รองรับ MFA ให้จำกัดการเข้าถึงด้วยการกำหนดแหล่งที่มา IP ที่ได้รับอนุญาต	☑
		ตรวจสอบและจำกัดการเข้าถึงระบบพัฒนา ระบบทดสอบ และระบบ staging ที่สามารถเข้าถึงได้จากอินเทอร์เน็ต รวมถึงส่วนบริหารจัดการของระบบดังกล่าว โดยกำหนดมาตรการควบคุมการเข้าถึงอย่างเข้มงวด หรือแยกออกจากเครือข่ายภายนอกหากไม่จำเป็น	☐
		ทบทวนการตั้งค่าด้านความมั่นคงปลอดภัยของระบบคลาวด์ โดยเฉพาะทรัพยากรที่เปิดเผยสู่สาธารณะ การตั้งค่าสิทธิ์ที่เกินความจำเป็น และส่วนบริหารจัดการที่อาจเข้าถึงได้จากภายนอก	☐
2. มาตรการลด Attack Surface และจำกัดเส้นทางการโจมตี			
2	**มาตรการลด Attack Surface และจำกัดเส้นทางการโจมตี**	จัดทำและปรับปรุงบัญชีทรัพย์สินสารสนเทศ (Asset Inventory) ให้ครบถ้วนและเป็นปัจจุบัน เพื่อให้สามารถมองเห็นจุดเสี่ยงภายในองค์กรได้อย่างต่อเนื่อง	☐
		ลดการเปิดเผยบริการที่ไม่จำเป็นสู่ภายนอก โดยปิดพอร์ต โปรโตคอล และบริการที่ไม่ได้ใช้งาน พร้อมปรับการตั้งค่าความปลอดภัยของระบบ (Hardening)	☐
		ดำเนินการแบ่งส่วนเครือข่าย (Network Segmentation) เพื่อลดความสามารถในการเคลื่อนย้ายภายในเครือข่ายจากผู้โจมตี (Lateral Movement)	☐
		ตรวจสอบซอฟต์แวร์ที่มีการพึ่งพาจากผู้ให้บริการภายนอกและประเมินความเสี่ยงจากผู้ให้บริการอย่างสม่ำเสมอ	☐

3. มาตรการเฝ้าระวังและตรวจจับ			
3	มาตรการเฝ้าระวังและตรวจจับ	จัดให้มีการเฝ้าระวังเส้นทางโจมตีที่สำคัญอย่างต่อเนื่อง ครอบคลุมระบบ เครือข่าย และบัญชีสิทธิ์สูง	☐
		จัดเก็บและวิเคราะห์บันทึกเหตุการณ์ (Log) จากหลายแหล่ง เพื่อสนับสนุนการตรวจจับและตอบสนองเหตุการณ์ได้อย่างทันท่วงที	☐
4. มาตรการเสริมการป้องกันของระบบ			
4	มาตรการเสริมการป้องกันของระบบ	ใช้แนวทางการป้องกันแบบหลายชั้น (Defence-in-Depth) เช่น Firewall/IPS, MFA, Network Segmentation และ Endpoint Detection and Response (EDR)	☐
		บูรณาการมาตรการด้านความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบและซอฟต์แวร์ ตามแนวทาง Secure Software Development Life Cycle (Secure SDLC)	☐
		พิจารณานำแนวคิด Zero Trust Architecture มาใช้ เพื่อเสริมการควบคุมการเข้าถึงและการตรวจสอบอย่างต่อเนื่อง	☐
5. มาตรการบริหารจัดการช่องโหว่และการแก้ไข			
5	มาตรการบริหารจัดการช่องโหว่และการแก้ไข	เพิ่มความถี่ในการตรวจสอบช่องโหว่และติดตามผลการแก้ไขอย่างใกล้ชิด โดยเฉพาะช่องโหว่ที่มีความเสี่ยงสูง	☐
		ปรับปรุงกระบวนการตรวจสอบและติดตั้ง Patch ให้ทันสมัย เพื่อลดช่วงเวลาที่ระบบอยู่ในภาวะเสี่ยง	☐
6. มาตรการตอบสนองและฟื้นฟู			
6	มาตรการตอบสนองและฟื้นฟู	จัดทำและทบทวนแผนตอบสนองเหตุการณ์ (Incident Response Plan) ให้รองรับสถานการณ์โจมตีที่ซับซ้อน	☑
		ซักซ้อมการตอบสนองเหตุการณ์และการฟื้นฟูระบบอย่างสม่ำเสมอ	☐
		จัดให้มีการสำรองข้อมูลตามหลัก 3-2-1 Backup และแยกเก็บข้อมูลสำรองออกจากระบบหลัก	☑
7. มาตรการเชิงกลยุทธ์ในยุค AI			
7	มาตรการเชิงกลยุทธ์ในยุค AI	ทบทวนสมมติฐานด้านภัยคุกคาม โดยคำนึงถึงผู้โจมตีที่อาจใช้ AI เพิ่มขีดความสามารถในการโจมตี	☐
		พิจารณานำ AI มาช่วยสนับสนุนการตรวจจับภัยคุกคาม วิเคราะห์ช่องโหว่ และประเมินความเสี่ยง	☐
		กำหนดแนวทางกำกับดูแลการใช้งาน AI อย่างเหมาะสม โดยยังคงมีผู้เชี่ยวชาญกำกับดูแลในจุดตัดสินใจที่สำคัญ	☐

หมายเหตุ / ข้อจำกัด: .....

.....

.....

.....

.....

.....

ลงชื่อ.....

(.....)

ตำแหน่ง.....

วันที่ ๒๑ / พ.ค. / 2569

(หัวหน้าหน่วยงาน หรือผู้รับมอบอำนาจ)