



ที่ ศธ ๐๗๐๔๕.๐๖/ ๓๕๖

ศูนย์ส่งเสริมการเรียนรู้ระดับอำเภอบ่อไร่
ถนนเทศบาล ๒ ตำบลบ่อพลอย อำเภอบ่อไร่
จังหวัดตราด ๒๓๑๔๐

๒๗ พฤษภาคม ๒๕๖๙

เรื่อง แนวทางการป้องกันและคำแนะนำการรับมือภัยคุกคามจากโมเดลปัญญาประดิษฐ์ (AI)

เรียน ผู้อำนวยการสำนักงานส่งเสริมการเรียนรู้ประจำจังหวัดตราด

อ้างถึง หนังสือสำนักงานสกร.ประจำจังหวัดตราด ที่ศธ ๐๗๐๔๕/ว ๘๙๒ ลงวันที่ ๑๙ พฤษภาคม ๒๕๖๙

สิ่งที่ส่งมาด้วย ๑.แบบตอบรับการตรวจสอบแนวทางการรับมือกรณี AI ๑ จำนวน ๑ เล่ม

ตามหนังสือ ที่ศธ ๐๗๐๔๕/ว ๘๙๒ ลงวันที่ ๑๙ พฤษภาคม ๒๕๖๙ สำนักงานส่งเสริมการเรียนรู้
ประจำจังหวัดตราดแจ้งศูนย์ส่งเสริมการเรียนรู้ระดับอำเภอบ่อไร่ดำเนินรับทราบและนำแนวทางการป้องกันและ
คำแนะนำการรับมือภัยคุกคามจากโมเดลปัญญาประดิษฐ์ (AI) ที่เกี่ยวข้องโดยเร่งด่วนตามความละเอียดแจ้งแล้วนั้น

ศูนย์ส่งเสริมการเรียนรู้ระดับอำเภอบ่อไร่ ขอรายงานผลการดำเนินงาน ดังกล่าวเรียบร้อยแล้วตาม
เอกสารที่แนบพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ

(นายชยธร วัชรพงศ์ศิริ)

ผู้อำนวยการศูนย์ส่งเสริมการเรียนรู้ระดับอำเภอเกาะช้าง
รักษาการในตำแหน่ง ผู้อำนวยการศูนย์ส่งเสริมการเรียนรู้ระดับอำเภอบ่อไร่

กลุ่มอำนวยการ งานบุคลากร

โทรศัพท์ ๐ ๓๙๕๙ ๑๕๔๐

แผนให้ตอบสนองเหตุการณ์ Incident Response Plan ให้ครอบคลุมสถานการณ์การโจมตีโดยใช้ AI เป็นเครื่องมือ และกำหนดผู้รับผิดชอบแต่ละขั้นตอน

ขั้นตอน	แนวทางในการดำเนินงาน	ผู้รับผิดชอบ
๑. การป้องกัน (Prevention)	<ul style="list-style-type: none"> - กำหนดนโยบายการใช้ AI อย่างปลอดภัย - อบรมบุคลากรเรื่องภัยคุกคามจาก AI และ Cybersecurity - ติดตั้งโปรแกรมป้องกันไวรัสและระบบ Firewall - สำรองข้อมูลสำคัญเป็นประจำ 	ผู้อำนวยการศูนย์ส่งเสริมการเรียนรู้ระดับอำเภอ ครูผู้ดูแลระบบ เจ้าหน้าที่เทคโนโลยีอำเภอ
๒. การเฝ้าระวัง (Detection)	<ul style="list-style-type: none"> - ตรวจสอบอีเมล/ข้อความต้องสงสัยจาก AI Phishing - เฝ้าระวังการเข้าถึงข้อมูลผิดปกติ - ตรวจสอบการเผยแพร่ข้อมูลปลอมของหน่วยงาน 	เจ้าหน้าที่ เจ้าหน้าที่เทคโนโลยีอำเภอ บุคลากรทุกคน
๓. การตอบสนองเหตุการณ์ (Response)	<ul style="list-style-type: none"> - แยกอุปกรณ์ที่ถูกโจมตีออกจากเครือข่ายทันที - แจ้งผู้บริหารและผู้เกี่ยวข้อง - เก็บหลักฐานการโจมตี เช่น ภาพหน้าจอ อีเมล ลิงก์ 	ครูผู้ดูแลระบบ เจ้าหน้าที่เทคโนโลยีอำเภอ คณะทำงานความปลอดภัยข้อมูล
๔. การแก้ไขและฟื้นฟู (Recovery)	<ul style="list-style-type: none"> - กู้คืนข้อมูลจากระบบสำรอง - เปลี่ยนรหัสผ่านและตรวจสอบสิทธิ์การเข้าถึง - ตรวจสอบความปลอดภัยก่อนเปิดใช้งานระบบอีกครั้ง 	เจ้าหน้าที่ เจ้าหน้าที่เทคโนโลยีอำเภอ ผู้บริหารสถานศึกษา
๕. การสรุปและป้องกันซ้ำ (Lessons Learned)	<ul style="list-style-type: none"> - ประชุมสรุปเหตุการณ์และผลกระทบ - ปรับปรุงมาตรการรักษาความปลอดภัย - จัดทำรายงานและแนวทางการป้องกันเพิ่มเติม 	ผู้อำนวยการศูนย์ส่งเสริมการเรียนรู้ระดับอำเภอ คณะกรรมการ เจ้าหน้าที่เทคโนโลยีอำเภอ



ลงชื่อ.....
นางสาววิภาวี ทวีเกษม
เจ้าหน้าที่แผน



ลงชื่อ.....
นายชยธร วิชระพงษ์ศิริ
ผู้อำนวยการศูนย์ส่งเสริมการเรียนรู้ระดับอำเภอ
รักษาการในตำแหน่งผู้อำนวยการส่งเสริมการเรียนรู้ระดับอำเภอ

แบบตอบรับการตรวจสอบแนวทางการรับมือกรณี AI ถูกใช้เป็นเครื่องมือโจมตีทางไซเบอร์

(ตามหนังสือ สกมช. TLP: CLEAR)

หน่วยงาน: ศูนย์ส่งเสริมการค้าระหว่างประเทศ วันที่: ๒๗ / พค / ๒๕๖๕

แบบตอบรับการตรวจสอบแนวทางการรับมือกรณี AI ถูกใช้เป็นเครื่องมือโจมตีทางไซเบอร์			
ลำดับ	หัวข้อและแนวทางปฏิบัติ	รายละเอียดดำเนินการ	ดำเนินการเรียบร้อยแล้ว
1. มาตรการเร่งด่วน			
1	มาตรการเร่งด่วน	ตรวจสอบและแก้ไขช่องโหว่ โดยเฉพาะระบบที่เปิดให้บริการจากภายนอก เพื่อลดความเสี่ยงจากการถูกค้นหาและโจมตีโดยอัตโนมัติ	<input type="checkbox"/>
		บังคับใช้การพิสูจน์ตัวตนหลายปัจจัย (MFA) สำหรับบัญชีผู้ดูแลระบบ ระบบบริหารจัดการ อุปกรณ์สำคัญ และบริการคลาวด์ที่เกี่ยวข้อง ในกรณีที่ไม่มี MFA ให้จำกัดการเข้าถึงด้วยการกำหนดแหล่งที่มา IP ที่ได้รับอนุญาต	<input checked="" type="checkbox"/>
		ตรวจสอบและจำกัดการเข้าถึงระบบพัฒนา ระบบทดสอบ และระบบ staging ที่สามารถเข้าถึงได้จากอินเทอร์เน็ต รวมถึงส่วนบริหารจัดการของระบบดังกล่าว โดยกำหนดมาตรการควบคุมการเข้าถึงอย่างเข้มงวด หรือแยกออกจากเครือข่ายภายนอกหากไม่จำเป็น	<input type="checkbox"/>
		ทบทวนการตั้งค่าด้านความมั่นคงปลอดภัยของระบบคลาวด์ โดยเฉพาะทรัพยากรที่เปิดเผยแพร่สาธารณะ การตั้งค่าสิทธิ์ที่เกินความจำเป็น และส่วนบริหารจัดการที่อาจเข้าถึงได้จากภายนอก	<input type="checkbox"/>
2. มาตรการลด Attack Surface และจำกัดเส้นทางการโจมตี			
2	มาตรการลด Attack Surface และจำกัดเส้นทางการโจมตี	จัดทำและปรับปรุงบัญชีทรัพย์สินสารสนเทศ (Asset Inventory) ให้ครบถ้วนและเป็นปัจจุบัน เพื่อให้สามารถมองเห็นจุดเสี่ยงภายในองค์กรได้อย่างต่อเนื่อง	<input type="checkbox"/>
		ลดการเปิดเผยบริการที่ไม่จำเป็นสู่ภายนอก โดยปิดพอร์ต โปรโตคอล และบริการที่ไม่ได้ใช้งาน พร้อมปรับการตั้งค่าความปลอดภัยของระบบ (Hardening)	<input type="checkbox"/>
		ดำเนินการแบ่งส่วนเครือข่าย (Network Segmentation) เพื่อลดความสามารถในการเคลื่อนย้ายภายในเครือข่ายจากผู้โจมตี (Lateral Movement)	<input type="checkbox"/>
		ตรวจสอบซอฟต์แวร์ที่มีการพึ่งพาจากผู้ให้บริการภายนอก และประเมินความเสี่ยงจากผู้ให้บริการอย่างสม่ำเสมอ	<input type="checkbox"/>

3. มาตรการเฝ้าระวังและตรวจจับ		
3	มาตรการเฝ้าระวังและตรวจจับ	จัดให้มีการเฝ้าระวังเส้นทางโจมตีที่สำคัญอย่างต่อเนื่อง ครอบคลุมระบบ เครือข่าย และบัญชีสิทธิ์สูง <input type="checkbox"/>
		จัดเก็บและวิเคราะห์บันทึกเหตุการณ์ (Log) จากหลาย แหล่ง เพื่อสนับสนุนการตรวจจับและตอบสนองเหตุการณ์ ได้อย่างทัน่วงที <input type="checkbox"/>
4. มาตรการเสริมการป้องกันของระบบ		
4	มาตรการเสริมการป้องกันของระบบ	ใช้แนวทางการป้องกันแบบหลายชั้น (Defence-in-Depth) เช่น Firewall/IPS, MFA, Network Segmentation และ Endpoint Detection and Response (EDR) <input type="checkbox"/>
		บูรณาการมาตรการด้านความมั่นคงปลอดภัยตลอดวงจร ชีวิตของระบบและซอฟต์แวร์ ตามแนวทาง Secure Software Development Life Cycle (Secure SDLC) <input type="checkbox"/>
		พิจารณานำแนวคิด Zero Trust Architecture มาใช้ เพื่อ เสริมการควบคุมการเข้าถึงและการตรวจสอบอย่างต่อเนื่อง <input type="checkbox"/>
5. มาตรการบริหารจัดการช่องโหว่และการแก้ไข		
5	มาตรการบริหารจัดการช่องโหว่และ การแก้ไข	เพิ่มวุฒิในการตรวจสอบช่องโหว่และติดตามผลการ แก้ไขอย่างใกล้ชิด โดยเฉพาะช่องโหว่ที่มีความเสี่ยงสูง <input type="checkbox"/>
		ปรับปรุงกระบวนการตรวจสอบและติดตั้ง Patch ให้ ทันสมัย เพื่อลดเวลาที่ระบบอยู่ในภาวะเสี่ยง <input type="checkbox"/>
6. มาตรการตอบสนองและฟื้นฟู		
6	มาตรการตอบสนองและฟื้นฟู	จัดทำและทบทวนแผนตอบสนองเหตุการณ์ (Incident Response Plan) ให้รองรับสถานการณ์โจมตีที่ซับซ้อน <input checked="" type="checkbox"/>
		ซักซ้อมการตอบสนองเหตุการณ์และการฟื้นฟูระบบอย่าง สม่ำเสมอ <input type="checkbox"/>
		จัดให้มีการสำรองข้อมูลตามหลัก 3-2-1 Backup และแยก เก็บข้อมูลสำรองออกจากระบบหลัก <input checked="" type="checkbox"/>
7. มาตรการเชิงกลยุทธ์ในยุค AI		
7	มาตรการเชิงกลยุทธ์ในยุค AI	ทบทวนสมมติฐานด้านภัยคุกคาม โดยคำนึงถึงผู้โจมตีที่อาจ ใช้ AI เพิ่มขีดความสามารถในการโจมตี <input type="checkbox"/>
		พิจารณานำ AI มาช่วยสนับสนุนการตรวจจับภัยคุกคาม วิเคราะห์ช่องโหว่ และประเมินความเสี่ยง <input type="checkbox"/>
		กำหนดแนวทางกำกับดูแลการใช้งาน AI อย่างเหมาะสม โดยยังคงมีผู้เชี่ยวชาญกำกับดูแลในจุดตัดสินใจที่สำคัญ <input type="checkbox"/>

หมายเหตุ / ข้อจำกัด: _____

ลงชื่อ _____

นางนันทพร ธีรวิจิตรพงศ์

ตำแหน่ง ผอ. igit สกส.ร.ก. อวท. ๒๕๖

วันที่ ๒๓ / ๗ค / ๒๕๖๙

(หัวหน้าหน่วยงาน หรือผู้รับมอบอำนาจ)