แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

เตรียมพร้อมรับมือความเสี่ยงใหม่จาก AI ที่มีขีดความสามารถด้านไซเบอร์

วันที่แจ้งเตือน 24 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานความเสี่ยงด้านภัยคุกคามไซเบอร์ กรณีการพัฒนาการของเทคโนโลยีปัญญาประดิษฐ์ที่มีแนวโน้มส่งผลกระทบต่อภูมิทัศน์ภัยคุกคามทางไซเบอร์ โดยอาจส่งผลกระทบต่อสมดุลระหว่าง "ฝ่ายป้องกัน" และ "ฝ่ายโจมตี" ในโลกไซเบอร์อย่างมีนัยสำคัญ โดยเฉพาะเมื่อโมเดล AI มีขีดความสามารถในการช่วยค้นหาช่องโหว่ วิเคราะห์จุดอ่อนและเร่งกระบวนการพัฒนาแนวทางการโจมตีให้เกิดขึ้นได้รวดเร็วและซับซ้อนมากยิ่งขึ้นได้

รายละเอียดด้านความเสี่ยงและแนวโน้มภัยคุกคาม: Claude Mythos เป็นโมเดล AI ที่ถูกพัฒนาโดยบริษัท Anthropic ซึ่งมีความสามารถในการช่วยค้นหาช่องโหว่แบบ zero-day ในระบบปฏิบัติการและเว็บเบราว์เซอร์ รวมถึงสามารถช่วยสร้างหรือปรับปรุง exploit สำหรับโจมตีช่องโหวบางประเภทได้ นอกจากนี้สามารถจัดการช่องโหว่ที่มีความซับซ้อน เช่น use-after-free, race condition การข้ามกลไกป้องกันบางรูปแบบ และการค้นพบจุดอ่อนในซอฟต์แวร์ที่มีการใช้งานมานานโดยไม่ถูกตรวจพบมาก่อน

ผลกระทบที่อาจเกิดขึ้น:

- ทำให้การค้นหาช่องโหว่และการนำไปใช้โจมตีเกิดขึ้นได้รวดเร็วขึ้น
- เพิ่มแรงกดดันต่อทีมรักษาความมั่นคงปลอดภัยไซเบอร์ในการวิเคราะห์และตอบสนองต่อเหตุการณ์
- ทำให้ระบบเก่า ระบบที่มีช่องโหว่ทางเทคนิคสะสม หรือระบบที่มีการพึ่งพาซอฟต์แวร์จากหลายแหล่งมีความเสี่ยงมากขึ้น
- เพิ่มโอกาสที่ช่องโหว่หลายรายการจะถูกเชื่อมโยงเข้าด้วยกันเป็นห่วงโซ่การโจมตีที่ซับซ้อนกว่าเดิม
- กระทบต่อโครงสร้างพื้นฐานสำคัญและบริการดิจิทัลที่ประชาชนใช้ในชีวิตประจำวัน

แนวทางป้องกัน:

1. ปรับกลยุทธ์เชิงรุก: ทบทวนการประเมินความเสี่ยงและสมมติฐานด้านภัยคุกคามใหม่ เพื่อรับมือกับผู้โจมตีที่ใช้ AI พัฒนาการโจมตีได้รวดเร็วและซับซ้อนขึ้น
2. เฝ้าระวังรอบด้าน: เพิ่มขีดความสามารถในการมองเห็นทรัพย์สินดิจิทัลและช่องทางการโจมตี (Attack Surface) ทั้งหมด พร้อมติดตามความเสี่ยงแบบ Real-time
3. จัดการช่องโหว่อย่างรวดเร็ว: เพิ่มความถี่ในการตรวจสอบและแก้ไขช่องโหว่ โดยจัดลำดับความสำคัญจากความรุนแรงและโอกาสที่จะถูกโจมตีจริง
4. สร้างความยืดหยุ่น (Resilience): จำกัดความเสียหายด้วยการแบ่งส่วนเครือข่าย การจำกัดสิทธิ์ (Least Privilege) และสำรองข้อมูลตามหลัก 3-2-1 Backup โดยแยกเก็บจากระบบหลักเพื่อป้องกันการถูกลบทำลาย
5. ใช้ AI ป้องกัน: นำเทคโนโลยี AI มาช่วยเสริมศักยภาพด้านการป้องกัน แต่ต้องมีผู้เชี่ยวชาญ (Human-in-the-loop) กำกับดูแลในจุดสำคัญและมีแนวทางควบคุมที่เหมาะสม

นอกจากนี้ ThaiCERT ยังออก Checklist เพื่อให้บริษัทเตรียมความพร้อมรับมือต่อภัยคุกคามเพิ่มเติม ดังเอกสารแนบท้าย

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 24 เม.ย. 2569
2. https://www.anthropic.com/glasswing
3. https://www.picussecurity.com/resource/blog/anthropics-project-glasswing-paradox?

แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

เตรียมพร้อมรับมือความเสี่ยงใหม่จาก AI ที่มีขีดความสามารถด้านไซเบอร์

วันที่แจ้งเตือน 24 เมษายน 2569

เอกสารแนบ: Checklist เพื่อให้บริษัทเตรียมความพร้อมรับมือต่อภัยคุกคามเพิ่มเติม

มาตรการรับมือภัยคุกคาม	รายละเอียดและแนวทางปฏิบัติ
1. มาตรการเร่งด่วน	• ตรวจสอบและแก้ไขช่องโหว่ระบบที่เปิดให้บริการภายนอกทันที • บังคับใช้ MFA สำหรับบัญชีผู้ดูแลระบบและบริการคลาวด์ (หรือจำกัด IP หากไม่รองรับ) • จำกัดการเข้าถึงระบบพัฒนา/ทดสอบ (Staging) จากอินเทอร์เน็ตอย่างเข้มงวด • ทบทวนการตั้งค่าความปลอดภัย สิทธิ์ และการบริหารจัดการบน Cloud • ปรับปรุงสิทธิ์ให้เป็นไปตามหลัก Least Privilege และยกเลิกบัญชีที่ไม่ใช้งาน • เปิดใช้งาน DDoS Protection สำหรับระบบที่เปิดให้บริการภายนอก
2. การลด Attack Surface	• ปรับปรุงบัญชีทรัพย์สินสารสนเทศ (Asset Inventory) ให้เป็นปัจจุบันเสมอ • ปิดพอร์ต/บริการที่ไม่จำเป็นและดำเนินการ System Hardening • แบ่งส่วนเครือข่าย (Network Segmentation) เพื่อจำกัดการเคลื่อนย้ายของผู้โจมตี • ประเมินความเสี่ยงของซอฟต์แวร์และผู้ให้บริการภายนอก (Third-party) สม่ำเสมอ
3. การเฝ้าระวังและตรวจจับ	• เฝ้าระวังเส้นทางการโจมตีสำคัญต่อเนื่อง (ครอบคลุมระบบ, เครือข่าย, บัญชีสิทธิ์สูง) • จัดเก็บและวิเคราะห์บันทึกเหตุการณ์ (Logs) เพื่อการตรวจจับที่รวดเร็ว
4. การเสริมการป้องกัน	• ใช้แนวทางการป้องกันแบบหลายชั้น (Defence-in-Depth) • บูรณาการความปลอดภัยในวงจรการพัฒนาซอฟต์แวร์ (Secure SDLC) • นำแนวคิด Zero Trust มาใช้ในการควบคุมการเข้าถึงและตรวจสอบต่อเนื่อง
5. การบริหารจัดการช่องโหว่	• เพิ่มความถี่ในการตรวจสอบช่องโหว่ โดยเฉพาะจุดที่มีความเสี่ยงสูง • ลดช่วงเวลาเสี่ยงโดยปรับปรุงกระบวนการทดสอบและติดตั้ง Patch ให้รวดเร็วขึ้น
6. การตอบสนองและฟื้นฟู	• จัดทำและทบทวนแผน IR (Incident Response) ให้รองรับการโจมตีที่ซับซ้อน • ซักซ้อมแผนการตอบสนองและฟื้นฟูระบบอย่างสม่ำเสมอ • สำรองข้อมูลตามหลัก 3-2-1 Backup และแยกเก็บข้อมูลสำรองออกจากระบบหลัก
7. มาตรการเชิงกลยุทธ์ยุค AI	• ทบทวนภัยคุกคามโดยคำนึงถึงผู้โจมตีที่ใช้ AI เพิ่มขีดความสามารถในการโจมตี • นำ AI มาใช้สนับสนุนการตรวจจับ วิเคราะห์ช่องโหว่ และประเมินความเสี่ยง • กำหนดแนวทางกำกับดูแล AI โดยมีผู้เชี่ยวชาญตัดสินใจในจุดที่สำคัญ