

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

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



แจ้งเตือนเพื่อเฝ้าระวังเตรียมพร้อมรับมือภัยคุกคามไซเบอร์ในยุค AI

วันที่แจ้งเตือน 25 กันยายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานความเสี่ยงด้านภัยคุกคามไซเบอร์ กรณีพัฒนาการของเทคโนโลยีปัญญาประดิษฐ์ (AI) ที่ส่งผลกระทบต่อภูมิทัศน์ของภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง ซึ่งอาจกระทบต่อการให้บริการขององค์กรได้ ดังนี้

การโจมตี	กรณีศึกษา
AI ทำให้การโจมตีไซเบอร์เร็วขึ้นและแม่นยำขึ้น ส่งผลให้ระยะเวลาระหว่างการพบช่องโหว่กับการโจมตีจริงสั้นลงอย่างมาก เช่น - ค้นหาและวิเคราะห์ช่องโหว่ของระบบ - พัฒนาโค้ดหรือเครื่องมือโจมตี - สำรวจและระบุเป้าหมาย (Reconnaissance) - ปรับเปลี่ยนเทคนิคเพื่อหลบเลี่ยงการตรวจจับ - วิเคราะห์ข้อมูลจำนวนมากที่ถูกขโมยมาได้อย่างรวดเร็ว AI เพิ่มประสิทธิภาพการหลอกลวง (Social Engineering) - สร้างอีเมลฟิชชิ่งเฉพาะบุคคล (Spear Phishing) สร้างข้อความหลอกลวงที่น่าเชื่อถือ - ปลอมแปลงเสียง ภาพ และ วิดีโอ (Deepfake) แอบอ้างผู้บริหารหรือบุคคลที่น่าเชื่อถือหลอกให้เหยื่อเปิดเผยรหัสผ่าน ข้อมูลสำคัญ หรือดำเนินการทางการเงิน	AI กับการจารกรรมไซเบอร์ รายงานของ Anthropic พบการใช้ AI ในการ - สำรวจเครือข่าย พัฒนาและทดสอบโค้ดโจมตี รวบรวม Credential ขโมย และส่งข้อมูลออกจากองค์กร โดยพบว่ามีเครื่องมือโจมตีต้องกรหลายแห่งและบางกรณีสามารถเจาะระบบได้สำเร็จ AI สนับสนุนการโจมตีผ่าน Cloud และ SaaS - โดยมีการใช้ AI เพื่อค้นหาช่องโหว่ ใช้ Credential ที่รั่วไหลเข้าถึงข้อมูลบน Cloud ขยายผลจากผู้ให้บริการ SaaS ไปยังลูกค้า สะท้อนความเสี่ยงของ Supply Chain และ Third-party Service อย่างชัดเจน AI-Generated Voice Scam - FB/IC3 รายงานกรณีการใช้เสียงสังเคราะห์ด้วย AI แอบอ้างเจ้าหน้าที่ระดับสูงเพื่อหลอกให้เหยื่อคลิกลิงก์อันตราย เปลี่ยนช่องทางสื่อสาร เปิดเผยข้อมูลสำคัญ แสดงให้เห็นว่า "ความไว้วางใจของมนุษย์" กลายเป็นช่องโหว่สำคัญที่สุด
ความเสี่ยงที่องค์กรต้องเผชิญ: - เวลาป้องกันลดลง - ช่องโหว่ถูกนำไปใช้โจมตีได้รวดเร็วขึ้น - ระบบที่พึ่งพิงการถูกพบง่ายขึ้น - ระบบเก่า ระบบทดสอบ หรือบริการที่ไม่มีผู้ดูแลกลายเป็นเป้าหมายสำคัญ - Credential Leakage สร้างความเสียหายวงกว้าง - รหัสผ่านหรือ Token ที่รั่วไหลถูกใช้ขยายสิทธิ์ในระบบ - Supply Chain Risk เพิ่มขึ้น - ผู้ให้บริการรายหนึ่งถูกโจมตี อาจส่งผลกระทบต่อลูกค้าจำนวนมาก - การตรวจจับและตอบสนองมีเวลาน้อยลง - เพิ่มโอกาสเกิด Data Breach, Ransomware และระบบล่ม	
แนวทางป้องกันและลดผลกระทบ: - บริหารจัดการช่องโหว่ตามความเสี่ยง (Risk-Based Management) - ลด Attack Surface และทำทะเบียนทรัพย์สินดิจิทัลให้ครบถ้วน - บังคับใช้ MFA / Passkey / FIDO2 โดยเฉพาะบัญชีผู้ดูแลระบบ - ใช้หลัก Least Privilege และบทบาทสิทธิ์เป็นประจำ - แบ่งแยกเครือข่าย (Network Segmentation) และใช้การป้องกันหลายชั้นเพื่อลดโอกาส Lateral movement - ตรวจสอบความปลอดภัยของซอฟต์แวร์ตั้งแต่ขั้นตอนการพัฒนา และประเมินความเสี่ยงจากผู้ให้บริการภายนอกที่สามารถเข้าถึงระบบหรือข้อมูลขององค์กร	- เฝ้าระวังตรวจสอบ Log และเพิ่มความสามารถในการตรวจจับเหตุการณ์ผิดปกติ - สร้างความตระหนักรู้เรื่อง Phishing และ Deepfake - ฝึกซ้อม Incident Response อย่างสม่ำเสมอ - สำรองข้อมูลตามหลัก 3-2-1 และทดสอบการกู้คืนระบบเป็นประจำ - จัดทำนโยบายและกำกับดูแลการใช้งาน AI อย่างเหมาะสม ประเมินความเสี่ยงจากการโจมตี การเชื่อมต่อ AI กับบริการภายนอก กำหนดขอบเขตและสิทธิการเข้าถึงอย่างชัดเจน

ข้อมูลอ้างอิง

- รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 24 ก.ย. 2569
- <https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027?>
- <https://www.ic3.gov/PSA/2025/PSA251219?>
- <https://www.anthropic.com/threat-intelligence-report-september-2026>