แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

ผู้ไม่ประสงค์ดีใช้ AI Chatbot โจมตีทางไซเบอร์และขโมยข้อมูล

วันที่แจ้งเตือน 26 กุมภาพันธ์ 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานกรณีที่ผู้ไม่ประสงค์ดีใช้ AI Chatbot เป็นเครื่องมือสนับสนุนการโจมตีระบบสารสนเทศของหน่วยงานในต่างประเทศหลายแห่ง

จากรายงานดังกล่าวพบว่าผู้ไม่ประสงค์ดีได้ป้อนคำสั่ง (Prompt) ให้ระบบ AI ทำหน้าที่เสมือนเป็นผู้เชี่ยวชาญด้านการเจาะระบบ เพื่อช่วยค้นหาช่องโหว่ในเครือข่าย เขียนสคริปต์สำหรับใช้ประโยชน์จากช่องโหว่ดังกล่าว และออกแบบกระบวนการทำให้การขโมยข้อมูลสามารถดำเนินการแบบอัตโนมัติได้ ส่งผลให้มีการเข้าถึงและขโมยข้อมูลของหน่วยงานได้ ทั้งนี้ เหตุการณ์ดังกล่าวสะท้อนให้เห็นถึงแนวโน้มที่ผู้ไม่ประสงค์ดีจะใช้เทคโนโลยีปัญญาประดิษฐ์เป็นเครื่องมือเสริมศักยภาพการโจมตี (AI-assisted cyber attack) ได้สำเร็จเพิ่มขึ้น

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจพิจารณาทบทวนการดำเนินการมาตรการ Cybersecurity ให้มีประสิทธิภาพอย่างสม่ำเสมอ ได้แก่

- ทบทวนนโยบายการใช้งานระบบปัญญาประดิษฐ์ (AI Usage Policy) ภายในองค์กร รวมถึงกำหนดขอบเขตการใช้งานที่เหมาะสม
- เปิดใช้งาน Multi-Factor Authentication (MFA) สำหรับระบบสำคัญและบัญชีผู้ดูแลระบบ
- เฝ้าระวังพฤติกรรมการใช้งานระบบที่ผิดปกติ เช่น การเรียกใช้งานสคริปต์อัตโนมัติ การดึงข้อมูลจำนวนมากผิดปกติ หรือการเชื่อมต่อไปยังปลายทางที่ไม่คุ้นเคย เป็นต้น
- ทดสอบและประเมินช่องโหว่ระบบอย่างสม่ำเสมอ (Vulnerability Assessment / Penetration Testing)
- เสริมสร้างความตระหนักรู้แก่พนักงานเกี่ยวกับภัยคุกคามจาก Social Engineering และการใช้ AI
- ติดตามข่าวสารการแจ้งเตือนภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง

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

ข้อมูลอ้างอิง

1. https://cybersecuritynews.com/claude-ai-exploited-2/

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ