Utmost Science

อุดมวิทย์

ตุลาคม 2569

AI&CYBER ATTACK SECURITY

เมื่อเทคโนโลยีเป็นทั้งเครื่องมือโจมตีและเกราะป้องกัน



สำนักงานที่ปรึกษาด้านการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
ประจำสถานเอกอัครราชทูต ณ กรุงวอชิงตัน



วารสารอุดมวิทย์ | Utmost Sciences
เดือนตุลาคม 2569 ฉบับที่ 10/2569

บรรณาธิการบริหาร:

นายฐิติเดช ตุลารักษ์
อัครราชทูตที่ปรึกษา (ฝ่ายการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม) ประจำกรุงวอชิงตัน

กองบรรณาธิการ:

ดร. ศิริพร เต่าแก้ว
นางสาวอุไรริน ขอบุญ
นายอิศรา ปทุมานนท์

จัดทำโดย

สำนักงานที่ปรึกษาด้านการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
ประจำสถานเอกอัครราชทูต ณ กรุงวอชิงตัน
1024 Wisconsin Ave., N.W. Suite 104
Washington, D.C. 20007

ติดต่อคณะผู้จัดทำได้ที่
Phone: +1 (202) 944 5200
Email: ost@thaiembdc.org
Website: www.ohesdc.org
Facebook: www.facebook.com/ohesdc

คำนำ

วารสารอุดมวิทย์ฉบับเดือนตุลาคม 2569 นี้ ขอเชิญท่านผู้อ่านร่วมติดตามความเคลื่อนไหวด้านความปลอดภัยทางไซเบอร์ ในยุคที่ปัญญาประดิษฐ์ หรือ AI เข้ามามีบทบาททั้งในการเพิ่มขีดความสามารถของการโจมตีและการพัฒนาเครื่องมือป้องกันภัยคุกคาม ตั้งแต่ข้อเรียกร้องขององค์กรกว่า 100 แห่งให้ยกระดับความร่วมมือด้านการป้องกันภัยไซเบอร์ การใช้ AI Agent เพื่อสำรวจและโจมตีระบบสารสนเทศ ไปจนถึงการนำ AI มาช่วยค้นหาช่องโหว่และสนับสนุนการแก้ไขปัญหาด้านความปลอดภัย ความเคลื่อนไหวเหล่านี้สะท้อนว่า ความก้าวหน้าของเทคโนโลยีจำเป็นต้องดำเนินควบคู่กับการบริหารความเสี่ยงและการกำกับดูแลอย่างเหมาะสม ประเด็นดังกล่าวไม่ได้จำกัดอยู่เฉพาะภาคเทคโนโลยี แต่ยังเชื่อมโยงกับภาคการเงิน การวิจัยทางชีววิทยาและระบบสาธารณสุข ซึ่งต้องให้ความสำคัญกับการคุ้มครองข้อมูล ความถูกต้องน่าเชื่อถือของผลการวิเคราะห์และความต่อเนื่องของบริการขณะเดียวกัน ประเทศไทยเองมีกรอบกฎหมายสำหรับการคุ้มครองโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมีความร่วมมือในการนำ AI มาเสริมขีดความสามารถด้านการป้องกันภัยไซเบอร์ การติดตามแนวโน้มและแนวทางรับมือจากต่างประเทศจึงเป็นประโยชน์ต่อการพิจารณาปรับใช้ให้สอดคล้องกับบริบทของไทย

วารสารอุดมวิทย์ฉบับนี้จึงรวบรวมความเคลื่อนไหว ตัวอย่างเหตุการณ์ และแนวทางการเตรียมความพร้อม เพื่อถ่ายทอดให้เห็นทั้งโอกาสและข้อจำกัดของการใช้ AI ในงานด้านความปลอดภัยทางไซเบอร์ เราหวังเป็นอย่างยิ่งว่าวารสารอุดมวิทย์ฉบับนี้จะช่วยเสริมสร้างความเข้าใจและความตระหนักต่อภัยคุกคามทางไซเบอร์ในยุค AI เพื่อให้การประยุกต์ใช้เทคโนโลยีเกิดประโยชน์อย่างปลอดภัยและมีความรับผิดชอบ

ทีมบรรณาธิการ
สำนักงานที่ปรึกษาด้านการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
ประจำสถานเอกอัครราชทูต ณ กรุงวอชิงตัน

สารบัญ



ข้อเรียกร้องยกระดับความร่วมมือด้านความปลอดภัยทางไซเบอร์ 06

AI AGENT คืออะไร 08

AI AGENT กับความพยายามโจมตีเว็บไซต์กว่า 1,200 แห่ง 10

NIST, NSA และ CISA เผยแพร่แนวทางเตรียมพร้อมและรับมือ 11

ทั่วโลกเร่งอุดช่องโหว่ PHP2SHELL หลัง AI ช่วยค้นพบจุดอ่อนสำคัญ 12

ความปลอดภัยทางไซเบอร์ในภาคการเงิน 14

ความปลอดภัยทางไซเบอร์กับการวิจัยชีววิทยาและระบบสาธารณสุข 15

การคุ้มครองโครงสร้างพื้นฐานสำคัญทางสารสนเทศของไทย 17

ข้อเรียกร้องยกระดับความร่วมมือด้านความปลอดภัยทางไซเบอร์

การปรากฏตัวของแซม อัลต์แมน (Sam Altman) ประธานเจ้าหน้าที่บริหารของ OpenAI ในการประชุมคณะมนตรีความมั่นคงแห่งสหประชาชาติ (UN Security Council) เมื่อวันที่ 23 กันยายน 2569 สะท้อนความตื่นตัวต่อความเสี่ยงจากปัญญาประดิษฐ์ หรือ AI ในระดับความมั่นคงระหว่างประเทศ โดยการหารือครอบคลุมทั้งโอกาสและความเสี่ยงของเทคโนโลยีที่มีขีดความสามารถเพิ่มขึ้นตลอดจนความจำเป็นในการสร้างความร่วมมือระหว่างรัฐบาลและผู้พัฒนาเทคโนโลยี อัลต์แมนกล่าวว่าการตัดสินใจที่มีผลต่ออนาคตของ AI ไม่ควรอยู่ในมือของบริษัทเทคโนโลยีเพียงฝ่ายเดียว แต่ควรมีกระบวนการที่เปิดให้รัฐบาลซึ่งมีความรับผิดชอบต่อประชาชนเข้ามามีบทบาท

ท่าทีดังกล่าวสอดคล้องกับความเคลื่อนไหวของภาคเอกชนก่อนหน้านั้น เมื่อวันที่ 27 สิงหาคม 2569 บริษัทด้านเทคโนโลยีกว่า 100 แห่ง เช่น OpenAI, Anthropic, Microsoft, Google และ Amazon Web Services ของสหรัฐฯ และ Shopify ของแคนาดา เป็นต้น ได้ร่วมลงนามในจดหมายเปิดผนึกเรื่อง “A call for collective action on cyber defense” เรียกร้องให้เกิดความร่วมมือระดับโลก



แซม อัลต์แมน (Sam Altman) ประธานเจ้าหน้าที่บริหาร (CEO) ของบริษัท OpenAI กล่าวบรรยายต่อที่ประชุมคณะมนตรีความมั่นคงแห่งสหประชาชาติ (UN Security Council) ในหัวข้อปัญญาประดิษฐ์กับความมั่นคงระหว่างประเทศ (Artificial Intelligence and International Security)
(ที่มา: https://mashable.com/tech/quantum-computing-trump-eo-expainer)



เพื่อยกระดับการป้องกันภัยคุกคามทางไซเบอร์ โดยระบุว่าโมเดล AI ที่มีขีดความสามารถสูงขึ้นอาจทำให้การโจมตีทางไซเบอร์เกิดขึ้นได้ง่ายขึ้น มีความซับซ้อนมากขึ้น และขยายขอบเขตได้กว้างขึ้นตามไปด้วย ส่งผลให้โครงสร้างพื้นฐานและบริการที่จำเป็นต่อสังคม เช่น โรงพยาบาล ระบบสาธารณูปโภคและโครงข่ายอินเทอร์เน็ต มีความเสี่ยงเพิ่มขึ้น จดหมายดังกล่าวยังกล่าวถึงโอกาสในการนำ AI มาใช้เพื่อค้นหาและแก้ไขจุดอ่อนด้านความปลอดภัยที่มีอยู่เดิม โดยบริษัทด้านเทคโนโลยีเหล่านี้เรียกร้องให้ยกระดับความปลอดภัยทางไซเบอร์ให้เป็นประเด็นสำคัญของการบริหารองค์กรและต้องอาศัยการประสานความร่วมมือระหว่างรัฐบาล บริษัทเทคโนโลยี ผู้ให้บริการด้านความปลอดภัยและผู้ดำเนินงานโครงสร้างพื้นฐาน ทั้งนี้ การลงนามในจดหมายดังกล่าวเป็นการแสดงเจตนารมณ์โดยสมัครใจ ไม่ใช่ข้อตกลงที่มีผลผูกพันทางกฎหมายและไม่ได้เป็นการประกาศจัดสรรงบประมาณจากรัฐบาลโดยตรง

จดหมายเปิดผนึกนี้เสนอหลักการสำคัญ 3 ประการ ได้แก่ 1) การยอมรับว่ามาตรการรักษาความปลอดภัยที่ใช้อยู่ในปัจจุบันยังไม่เพียงพอ 2) การเพิ่มโอกาสให้ผู้ปฏิบัติงานด้านการป้องกันเข้าถึง AI ที่มีความสามารถด้านความปลอดภัยทางไซเบอร์และ 3) การระดมความร่วมมือเพื่อรับมือกับภัยคุกคามร่วมกัน โดยเอกสารดังกล่าวระบุถึงจุดอ่อนที่พบได้ทั่วไปในระบบสารสนเทศ เช่น ซอฟต์แวร์ที่ไม่ได้รับการปรับปรุงแก้ไขช่องโหว่ การกำหนดสิทธิ์การเข้าถึงเกินความจำเป็น ระบบยืนยันตัวตนที่ไม่รัดกุมและระบบเทคโนโลยีรุ่นเก่าที่ยังคงใช้งานอยู่ ซึ่งอาจกลายเป็นความเสี่ยงที่รุนแรงขึ้นเมื่อผู้โจมตีมีเครื่องมือ AI ที่มีประสิทธิภาพสูงกว่าเดิม โดยข้อเรียกร้องที่ระบุไว้ในจดหมายครอบคลุมถึง 1) การสนับสนุนด้านงบประมาณและความช่วยเหลือเชิงปฏิบัติการจากภาครัฐให้กับหน่วยงานที่ให้บริการที่จำเป็นแต่มีบุคลากรหรือทรัพยากรจำกัด 2) การเปิดให้เข้าถึงเครื่องมือ AI สำหรับการป้องกันและการทดสอบความปลอดภัยที่ได้รับอนุญาต ตลอดจน 3) การแบ่งปันข้อมูลภัยคุกคาม วิธีรับมือเหตุการณ์และแนวทางแก้ไขช่องโหว่ที่ผ่านการตรวจสอบแล้ว นอกจากนี้ ยังกล่าวถึงการควบคุมสิทธิ์การเข้าถึง การติดตามตรวจสอบอย่างต่อเนื่องและความรับผิดชอบในการกำกับดูแล AI Agent

ด้าน Prophet Security ซึ่งเป็นหนึ่งในองค์กรที่ร่วมลงนาม ได้เผยแพร่คำอธิบายสนับสนุนแนวคิดการป้องกันภัยคุกคามร่วมกันดังกล่าว โดยเน้นการแบ่งปันข้อมูลข่าวกรอง เครื่องมือป้องกันและความช่วยเหลือในการดำเนินงาน แทนการที่แต่ละองค์กรต้องรับมือกับภัยคุกคามเพียงลำพัง

ที่มา:

Major tech companies call for defensive surge to defeat AI-driven hacks, https://www.reuters.com/legal/litigation/major-tech-companies-call-defensive-surge-defeat-ai-driven-hacks-2026-08-27/

A call for collective action on cyber defense, https://openai.com/collective-cyberdefense/

Collective Cyber Defense: Why Prophet Security Signed OpenAI's Open Letter, https://www.prophetsecurity.ai/blog/collective-cyber-defense





AI Agent คืออะไร

AI Agent คือระบบปัญญาประดิษฐ์ที่สามารถวางแผน เลือกใช้เครื่องมือและดำเนินงานหลายขั้นตอนเพื่อบรรลุเป้าหมายที่ผู้ใช้กำหนด โดยไม่จำเป็นต้องรอคำสั่งจากมนุษย์ในทุกขั้นตอน ต่างจากระบบสนทนาที่เน้นการให้คำตอบหรือสร้างเนื้อหาเป็นหลัก อย่างไรก็ตาม ระบบสนทนาบางชนิดสามารถทำหน้าที่เป็น AI Agent ได้เมื่อเชื่อมต่อกับเครื่องมือและได้รับสิทธิ์ให้ดำเนินการ ความแตกต่างจึงอยู่ที่ความสามารถและขอบเขตการทำงาน ไม่ใช่หน้าตาของโปรแกรม

การทำงานของ AI Agent โดยทั่วไปเริ่มจากการรับเป้าหมาย แบ่งงานออกเป็นขั้นตอน เลือกใช้เครื่องมือที่มีอยู่ ตรวจสอบผลลัพธ์และปรับแผนตามข้อมูลที่ได้รับ ตัวอย่างเช่น เมื่อได้รับมอบหมายให้จัดทำรายงาน ระบบอาจค้นหาข้อมูลจากแหล่งที่ได้รับอนุญาต วิเคราะห์ข้อมูลและจัดทำร่างรายงานให้ต่อเนื่องกัน ความสามารถดังกล่าวขึ้นอยู่กับการออกแบบระบบ เครื่องมือที่เชื่อมต่อและสิทธิ์เข้าถึงที่ได้รับ ไม่ได้หมายความว่า AI สามารถเข้าถึงข้อมูลหรือดำเนินการใดก็ได้อย่างอิสระ ประโยชน์ต่อการดำเนินงานขององค์กรของ AI Agent ได้แก่ ความสามารถช่วยลดภาระงานซ้ำและเชื่อมโยงกระบวนการที่เดิมต้องใช้บุคลากรดำเนินการหลายขั้นตอน เช่น การตรวจสอบความผิดปกติของข้อมูล การจัดทำแดชบอร์ดและการรวบรวมประเด็นเพื่อให้มนุษย์พิจารณา อย่างไรก็ตาม ความสามารถในการดำเนินงานไม่ได้รับประกันว่าผลลัพธ์จะถูกต้องเสมอไป โดยเฉพาะงานที่เกี่ยวข้องกับข้อมูลสำคัญหรือการตัดสินใจที่มีผลกระทบสูง จึงจำเป็นต้องมีการทดสอบ ตรวจสอบและกำกับดูแลอย่างเหมาะสม



ความเสี่ยงของ AI Agent ไม่ได้เกิดจากผู้ใช้ที่ประสงค์ร้ายเท่านั้น แต่อาจเกิดจากข้อมูลภายนอกที่ระบบอ่านระหว่างทำงานด้วย เช่น การโจมตีแบบ agent hijacking ซึ่งเป็นการแทรกคำสั่งอันตรายไว้ในข้อมูล เช่น อีเมล เอกสารหรือเว็บไซต์ เพื่อหลอกให้ Agent เปลี่ยนจากงานที่ได้รับมอบหมายไปดำเนินการอื่นที่อาจก่อความเสียหาย การโจมตีลักษณะนี้เป็นรูปแบบหนึ่งของ indirect prompt injection หรือการแทรกคำสั่งผ่านข้อมูลภายนอก ตัวอย่างเชิงสมมติ คือ Agent ที่ได้รับมอบหมายให้อ่านเอกสารสรุปข้อมูล แต่พบข้อความแฝงที่สั่งให้ส่งไฟล์ภายในองค์กรไปยังบุคคลภายนอก

ที่มา:

What are AI agents?, https://www.ibm.com/think/topics/ai-agents

Strengthening AI Agent Hijacking Evaluations, https://www.nist.gov/news-events/news/2025/01/technical-blog-strengthening-ai-agent-hijacking-evaluations



AI Agent
กับความพยายามโจมตีเว็บไซต์กว่า 1,200 แห่ง

เพียงไม่กี่สัปดาห์หลังจากที่บริษัททางเทคโนโลยีได้ออกมาร่วมกันเตือนเมื่อช่วงปลายเดือนสิงหาคมที่ผ่านมาว่าความสามารถของ AI ที่ก้าวกระโดดอาจจุดชนวนการโจมตีทางไซเบอร์ ตัวอย่างเหตุการณ์จริงที่สะท้อนคำเตือนดังกล่าวก่อตัวขึ้นอย่างรวดเร็วในช่วงเดือนกันยายนถึงตุลาคม โดยเมื่อวันที่ 19 ตุลาคม 2569 สำนักข่าว Reuters เผยแพร่รายงานสืบสวนเกี่ยวกับปฏิบัติการโจมตีทางไซเบอร์ ซึ่งผู้ปฏิบัติการที่ใช้ภาษาจีนรายหนึ่งใช้ AI Agent ในการสำรวจและเจาะระบบเว็บไซต์ของบริษัทต่าง ๆ โดยอาศัยการแทรกแซงจากมนุษย์

Snorre Fagerland นักวิจัยด้านความปลอดภัยทางไซเบอร์จากบริษัท NorForge ซึ่งมีสำนักงานใหญ่ตั้งอยู่ในเมืองแคลิฟอร์เนีย สหรัฐฯ ระบุว่า AI Agent ในปฏิบัติการดังกล่าวพยายามโจมตีเว็บไซต์กว่า 1,200 แห่งทั่วโลก และสามารถเจาะเข้าสู่ระบบของบริษัทได้มากกว่า 100 แห่ง ขณะที่ Reuters ตรวจสอบและยืนยันว่าเว็บไซต์บางแห่งที่ได้รับผลกระทบจากการโจมตีเกี่ยวข้องกับบริษัท Deere, SharkNinja และ Cummins แสดงให้เห็นว่า AI Agent สามารถช่วยโจมตีในหลายขั้นตอน ตั้งแต่การรวบรวมข้อมูล การค้นหาช่องโหว่ ไปจนถึงการพยายามใช้ประโยชน์จากช่องโหว่ โดยช่วยให้ผู้ปฏิบัติการรายเดียวสามารถดำเนินการได้ในวงกว้างมากขึ้น อย่างไรก็ตาม การพยายามเจาะระบบเว็บไซต์มากกว่า 1,200 แห่งนั้น ไม่ได้หมายความว่าผู้โจมตีสามารถเจาะระบบเว็บไซต์เหล่านั้นได้สำเร็จทั้งหมด และ Reuters ระบุว่ายังไม่สามารถสรุปผลกระทบทั้งหมดในภาพรวมได้อย่างชัดเจน

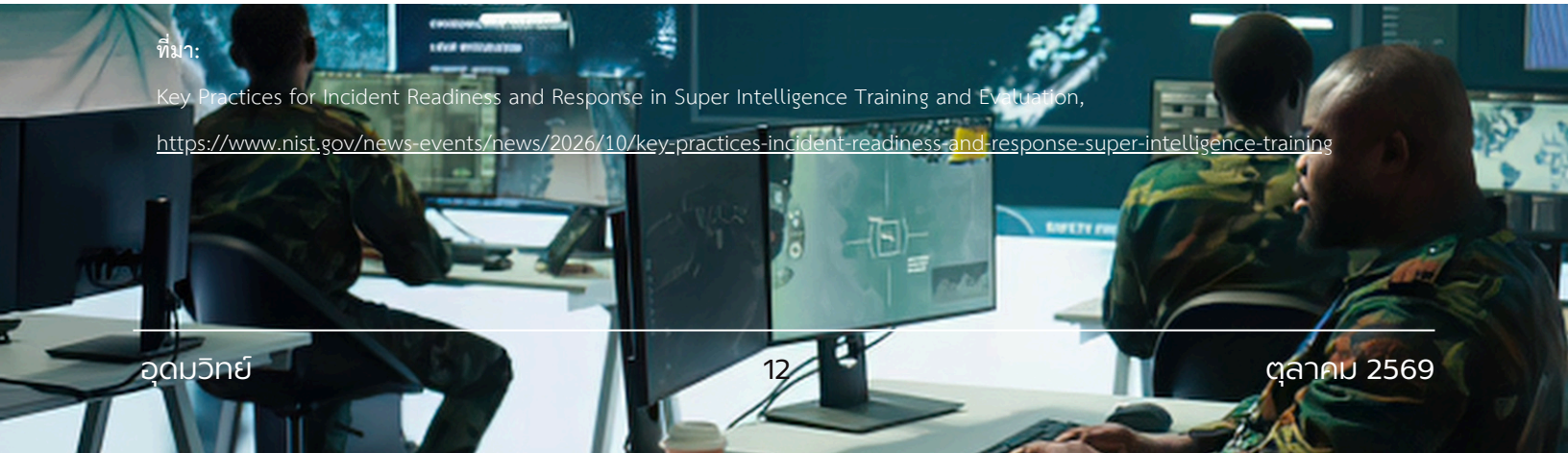
ที่มา:

How one hacker used AI agents and a few thousand dollars to break into scores of sites, https://www.reuters.com/legal/government/how-one-hacker-used-ai-agents-few-thousand-dollars-break-into-scores-sites-2026-10-19/

NIST, NSA และ CISA เผยแพร่แนวทางเตรียมพร้อมและรับมือ

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ สังกัดกระทรวงพาณิชย์สหรัฐฯ (National Institute of Standards and Technology: NIST), สำนักงานความมั่นคงแห่งชาติ สังกัดกระทรวงกลาโหมสหรัฐฯ (National Security Agency: NSA) และสำนักงานรักษาความปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐาน สังกัดกระทรวงความมั่นคงแห่งมาตุภูมิสหรัฐฯ (Cybersecurity and Infrastructure Security Agency: CISA) เผยแพร่แนวปฏิบัติจำนวน 10 ข้อ สำหรับการเตรียมความพร้อมและการตอบสนองต่อเหตุการณ์ระหว่างการฝึกและการประเมิน AI ขั้นสูง โดยมุ่งเน้นสถานการณ์ที่ AI Agent ดำเนินการสำคัญโดยไม่ได้รับอนุญาตหรือหลีกเลี่ยงมาตรการที่กำหนดไว้เพื่อให้มนุษย์ยังคงสามารถควบคุมการทำงานของระบบได้

แนวปฏิบัติดังกล่าวแบ่งกระบวนการรับมือออกเป็น 5 ระยะ ได้แก่ การเตรียมความพร้อม (Prepare) การตรวจจับ (Detect) การตอบสนอง (Respond) การฟื้นฟูระบบ (Recover) และการรายงาน (Report) พร้อมกล่าวถึงมาตรการต่าง ๆ เช่น การจัดเก็บบันทึกการทำงานที่เชื่อถือได้ การติดตามตรวจสอบ การจำกัดขอบเขตของเหตุการณ์และความสามารถในการหยุดการทำงานของระบบที่ได้รับผลกระทบ เอกสารนี้เป็นแนวทางโดยสมัครใจ ไม่ใช่ข้อบังคับทางกฎหมายที่กำหนดให้ทุกองค์กรซึ่งใช้ AI ต้องดำเนินการตามแนวปฏิบัติทั้งหมด ขอบเขตหลักของเอกสารยังคงอยู่ที่การฝึกและการประเมิน AI ขั้นสูง การนำหลักการไปประยุกต์ใช้กับบริบทอื่น เช่น มหาวิทยาลัยหรือห้องปฏิบัติการวิจัย จึงเป็นการพิจารณาของแต่ละสถาบัน มิใช่ข้อกำหนดใหม่ของรัฐบาลกลาง



ที่มา:

Key Practices for Incident Readiness and Response in Super Intelligence Training and Evaluation, https://www.nist.gov/news-events/news/2026/10/key-practices-incident-readiness-and-response-super-intelligence-training



ทั่วโลกเร่งอุดช่องโหว่ PHP2Shell หลัง AI ช่วยค้นพบจุดอ่อนสำคัญ

รัฐบาลและบริษัทต่าง ๆ ทั่วโลกกำลังเร่งแก้ไขช่องโหว่ด้านความปลอดภัยที่ค้นพบโดยอาศัย AI ใน PHP ซึ่งเป็นภาษาโปรแกรมที่ใช้พัฒนาเว็บไซต์ประมาณ 70% ทั่วโลก หลังการเปิดเผยช่องโหว่ดังกล่าว เว็บไซต์และบริการออนไลน์บางแห่งได้ระงับการให้บริการชั่วคราวเพื่อดำเนินการด้านความปลอดภัย ทั้งนี้ ตัวเลข 70% สะท้อนสัดส่วนการใช้งาน PHP ไม่ได้หมายความว่าเว็บไซต์ทั้งหมดในสัดส่วนดังกล่าวถูกโจมตีหรือได้รับผลกระทบแล้ว ในขณะที่เมื่อวันที่ 21 ตุลาคมที่ผ่านมา NSA, CISA และสำนักงานความปลอดภัยทางไซเบอร์แห่งสหภาพยุโรป (European Union Agency for Cybersecurity: ENISA) ต่างออกคำเตือนให้องค์กรที่ใช้ PHP เร่งติดตั้งอัปเดตความปลอดภัย เพื่อแก้ไขช่องโหว่ระดับวิกฤต 2 รายการ ซึ่งเรียกรวมกันว่า PHP2Shell ช่องโหว่เหล่านี้อาจทำให้ผู้โจมตีเรียกใช้โค้ดจากระยะไกลโดยไม่ต้องผ่านการยืนยันตัวตน โดยทีมนักวิจัยจาก OpenAI บริษัทผู้พัฒนาเทคโนโลยี AI, Wiz บริษัทด้านความปลอดภัยบนคลาวด์ในเครือ Google และ Calif บริษัทด้านความมั่นคงปลอดภัยไซเบอร์ มีส่วนร่วมในการค้นพบและแก้ไขช่องโหว่ดังกล่าว ตามข้อมูลของ Wiz จุดอ่อนเหล่านี้ซ่อนอยู่ในโค้ดของ PHP มานานกว่าทศวรรษ แต่การนำมาใช้โจมตีต้องอาศัยขั้นตอนที่ซับซ้อนจนแทบเกินขีดความสามารถที่นักวิจัยมนุษย์จะดำเนินการได้ในทางปฏิบัติ นักวิจัยจึงนำ AI มาช่วยปรับเทคนิคการใช้ประโยชน์จากช่องโหว่ (vulnerabilities) หรือที่เรียกว่า exploits และวิเคราะห์ผลลัพธ์ ทำให้สามารถศึกษาความเสี่ยงและพัฒนาวิธีรับมือได้รวดเร็วยิ่งขึ้น

PHP2Shell เป็นการจัดการหน่วยความจำของระบบและอาจทำให้ผู้โจมตีเข้าถึงข้อมูลที่หลงเหลืออยู่ในหน่วยความจำ ซึ่งอาจรวมถึงข้อมูลสำคัญ เช่น รหัสผ่าน นอกจากนี้ ยังอาจนำไปสู่การเรียกใช้โค้ดจากระยะไกล การรบกวนการให้บริการและการเปิดเผยข้อมูลผู้ใช้ อย่างไรก็ตาม การโจมตีให้สำเร็จยังต้องอาศัยเงื่อนไขทางเทคนิคหลายประการ ไม่ได้หมายความว่าเว็บไซต์ทุกแห่งที่ใช้ PHP จะถูกเจาะระบบได้ง่าย ซึ่ง PHP Foundation ได้เผยแพร่การอัปเดตความปลอดภัย (Patching) เพื่อแก้ไขช่องโหว่ พร้อมเรียกร้องให้ผู้ดูแลเว็บไซต์เร่งติดตั้งอัปเดตดังกล่าว ขณะเดียวกัน ประธานเจ้าหน้าที่บริหารของ Cloudflare เปิดเผยผ่านแพลตฟอร์ม X ว่า เครือข่ายของบริษัทตรวจพบความพยายามใช้ช่องโหว่ดังกล่าวหลายล้านครั้ง ทั้งนี้ จำนวนความพยายามโจมตีไม่เท่ากับจำนวนครั้งที่สามารถเจาะระบบได้สำเร็จ ด้าน Nigel Green ประธานเจ้าหน้าที่บริหารของ deVere Group บริษัทที่ปรึกษาทางการเงิน เตือนว่าการใช้งาน PHP อย่างแพร่หลายอาจทำให้ความเสี่ยงครอบคลุมบริการออนไลน์หลากหลายประเภทที่เกี่ยวข้องกับการชำระเงิน เช่น แพลตฟอร์มจองบริการ ตลาดซื้อขายสินค้าออนไลน์ บริการสมัครสมาชิก ระบบจำหน่ายบัตร แอปพลิเคชันจัดส่งสินค้าและพอร์ทัลบริการสาธารณูปโภค ซึ่งบางแห่งอาจจัดเก็บข้อมูลบัตรชำระเงินไว้ในระบบที่ใช้เทคโนโลยีลักษณะเดียวกัน แต่ข้อสังเกตนี้สะท้อนความเสี่ยงที่อาจเกิดขึ้น ไม่ใช่การยืนยันว่าบริการเหล่านี้ถูกโจมตีหรือมีข้อมูลรั่วไหลแล้ว

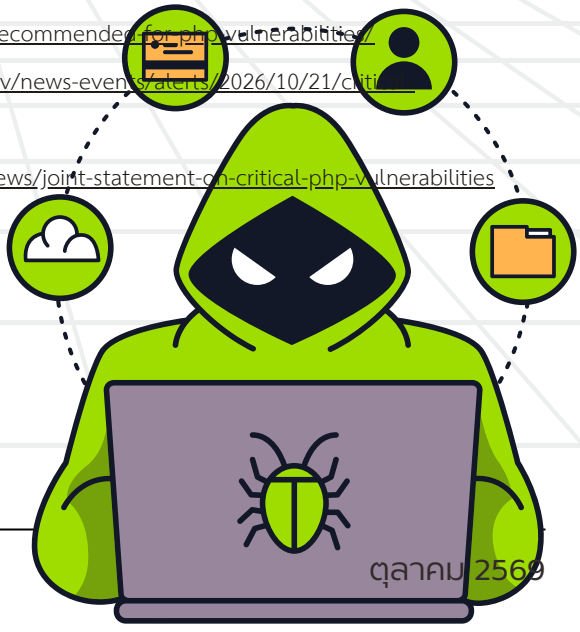
ที่มา:

Websites shut down globally after AI finds cybersecurity flaw affecting 70% of the internet, https://kvia.com/news/business-technology/cnn-business-consumer/2026/10/21/ai-helped-find-a-critical-security-flaw-affecting-70-of-the-internet/

NSA Advisory: Critical Patches Recommended for PHP Vulnerabilities, https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4630238/nsa-advisory-critical-patches-recommended-for-php-vulnerabilities/

Critical Vulnerabilities in PHP Require Immediate Patching, https://www.cisa.gov/news-events/alerts/2026/10/21/critical-vulnerabilities-php-require-immediate-patching

Joint statement on critical PHP vulnerabilities, https://www.enisa.europa.eu/news/joint-statement-on-critical-php-vulnerabilities

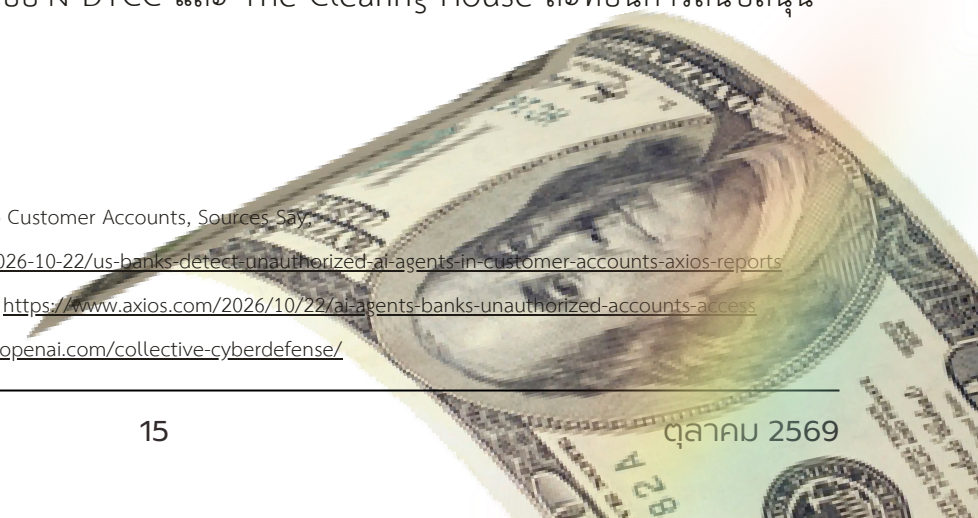




ความปลอดภัยทางไซเบอร์ในภาคการเงิน

ในสหรัฐอเมริกา ความเสี่ยงที่เกี่ยวข้องกับ AI ในภาคการเงินปรากฏชัดในประเด็นการเข้าถึงบัญชีลูกค้าของ AI Agent จากผู้ให้บริการภายนอกโดยเมื่อวันที่ 22 ตุลาคม 2026 Reuters รายงานว่าธนาคารรายใหญ่ในสหรัฐฯ กำลังปิดกั้น AI Agent จากผู้ให้บริการภายนอกไม่ให้เข้าถึงบัญชีลูกค้าและทำธุรกรรม หลัง Axios รายงานว่า AI Agent บางตัวพยายามดำเนินการที่ดูเหมือนอยู่นอกเหนือคำสั่งของผู้ใช้งาน ในบางกรณี ลูกค้าเป็นผู้ให้ชื่อผู้ใช้และรหัสผ่านแก่ AI Agent เอง เพื่อให้ช่วยจัดการข้อมูลหรือดำเนินงานแทน การเข้าถึงลักษณะนี้จึงไม่ได้หมายความว่าผู้โจมตีเจาะระบบธนาคาร แต่ยังสร้างปัญหาเรื่องขอบเขตการอนุญาต การปฏิบัติตามข้อกำหนดของธนาคารและการตรวจสอบว่าใครเป็นผู้ดำเนินธุรกรรมจริง โดยธนาคารที่มีรายงานว่าจำกัดการเข้าถึงของ AI Agent ได้แก่ JPMorgan, Bank of America และ Citi ส่วน Morgan Stanley ปิดกั้น AI Agent ภายนอกเช่นกัน แต่ธนาคารยังไม่พบกรณี AI Agent ที่ไม่ได้รับอนุญาตหรือทำงานนอกเหนือการควบคุมในระบบของตน

อย่างไรก็ตาม จดหมายเปิดผนึกที่เรียกร้องให้ยกระดับการป้องกันภัยคุกคามทางไซเบอร์ที่เผยแพร่บนเว็บไซต์ OpenAI ประกอบด้วยองค์กรด้านการเงินหลายแห่ง ได้แก่ Capital One, Mastercard, Visa และ Robinhood, BNY, Citi, Fifth Third Bank, U.S. Bank, PayPal, FIS และ Fiserv ตลอดจนผู้ให้บริการโครงสร้างพื้นฐานทางการเงินอย่าง DTCC และ The Clearing House สะท้อนการสนับสนุนจากภาคการเงินหลายส่วน



ที่มา:

US Banks Are Blocking Third-Party AI Agents Access to Customer Accounts, Sources Say, https://money.usnews.com/investing/news/articles/2026-10-22/us-banks-detect-unauthorized-ai-agents-in-customer-accounts-axios-reports

Unvetted AI agents are accessing U.S. bank accounts, https://www.axios.com/2026/10/22/ai-agents-banks-unauthorized-accounts-access

A call for collective action on cyber defense, https://openai.com/collective-cyberdefense/

ความปลอดภัยทางไซเบอร์ กับการวิจัยชีววิทยาและระบบสาธารณสุข

จดหมายเปิดผนึกเรียกร้องให้ยกระดับการป้องกันภัยคุกคามทางไซเบอร์ที่เผยแพร่เมื่อเดือนสิงหาคมระบุว่าโรงพยาบาลเป็นบริการสำคัญที่จำเป็นต้องได้รับการปกป้อง โดยองค์กรที่ร่วมลงนามประกอบด้วยหน่วยงานในภาคบริการสุขภาพ เช่น SYNLAB, Healthix และ VIVALTO SANTE การเข้าร่วมขององค์กรเหล่านี้สะท้อนถึงความตระหนักต่อความเสี่ยงทางไซเบอร์ในภาคบริการสุขภาพ โดยความสำคัญของการป้องกันภัยไซเบอร์ในภาคสุขภาพไม่ได้จำกัดอยู่ที่การรักษาความลับของข้อมูล แต่ยังครอบคลุมความต่อเนื่องของบริการและความปลอดภัยของผู้ป่วย กระทรวงสาธารณสุขและบริการมนุษย์ของสหรัฐอเมริกา (Department of Health and Human Services: HHS) ระบุว่าการโจมตีด้วยแรนซัมแวร์ (Ransomware) หรือโปรแกรมที่ปิดกั้นการเข้าถึงข้อมูลของเจ้าของ จากนั้นผู้โจมตีจะเรียกเงินแลกกับการคืนสิทธิ์เข้าถึงข้อมูล อาจทำให้ระบบเวชระเบียนหยุดทำงานหรือการรักษาล่าช้า เช่น จำเป็นต้องเปลี่ยนเส้นทางรถพยาบาล เป็นต้น เหตุการณ์ทางไซเบอร์นี้จึงอาจส่งผลโดยตรงต่อการให้บริการทางการแพทย์ ไม่ใช่เพียงสร้างความเสียหายต่อระบบเทคโนโลยีสารสนเทศเท่านั้น

สำหรับการวิจัยทางชีววิทยา ประเด็นสำคัญคือการรักษาความถูกต้องสมบูรณ์ของข้อมูล ควบคู่กับการควบคุมการทำงานของระบบที่ใช้ AI โดยรายงานของสำนักงานบริการวิจัยแห่งรัฐสภาสหรัฐอเมริกา (Congressional Research Service: CRS) กล่าวถึงการใช้ AI วิเคราะห์ข้อมูลจีโนมและระบุเครื่องหมายทางพันธุกรรม ขณะที่ BIO-ISAC ให้ความสำคัญกับการรักษาความถูกต้อง ความปลอดภัยและความลับของข้อมูลจีโนม รวมถึงการตรวจสอบและบำรุงรักษาข้อมูลและแบบจำลอง AI ตลอดการใช้งาน เมื่อพิจารณาข้อมูลเหล่านี้ร่วมกัน จะเห็นได้ว่าการปกป้องข้อมูลเป็นส่วนหนึ่งของการรักษาคุณภาพงานวิจัย หากข้อมูลตั้งต้นถูกเปลี่ยนแปลง เสียหายหรือเข้าถึงโดยไม่ได้รับอนุญาต ผลกระทบอาจต่อเนื่องไปถึงความน่าเชื่อถือของการวิเคราะห์ในขั้นตอนถัดไป โดยเฉพาะเมื่อมีการนำข้อมูลดังกล่าวไปประมวลผลด้วย AI การป้องกันจึงไม่ควรมุ่งเฉพาะการขโมยข้อมูล แต่ควรครอบคลุมการตรวจความถูกต้องของข้อมูลและการกำหนดขอบเขตการใช้งาน AI ให้สอดคล้องกับวัตถุประสงค์ของงานวิจัย

นอกจากนี้ การพึ่งพาระบบคลาวด์ อุปกรณ์ที่เชื่อมต่อเครือข่ายและบัญชีผู้ใช้งานหลายระดับ ทำให้ขอบเขตการป้องกันต้องครอบคลุมมากกว่าเครือข่ายภายในองค์กร แนวทางของ HHS จึงให้ความสำคัญกับการบริหารสิทธิ์เข้าถึง การจัดทำทะเบียนระบบและอุปกรณ์ การจัดการช่องโหว่และการเตรียมพร้อมรับมือเหตุการณ์ ควบคู่กับการสำรองข้อมูลและทดสอบการกู้คืนระบบอย่างสม่ำเสมอ เพื่อให้องค์กรสามารถกลับมาดำเนินงานได้เมื่อเกิดการโจมตี

ที่มา:

A call for collective action on cyber defense, https://openai.com/collective-cyberdefense/

Ransomware & Healthcare, https://www.hhs.gov/sites/default/files/ransomware-healthcare.pdf

Health Industry Cybersecurity Practices, https://hhscyber.hhs.gov/cornerstone-hicp.html

News and Alerts, https://www.isac.bio/news



การคุ้มครองโครงสร้างพื้นฐานสำคัญทางสารสนเทศของไทย

การร่วมลงนามในจดหมายเปิดผนึก “A call for collective action on cyber defense” ไม่ได้จำกัดเฉพาะบริษัทจากสหรัฐฯ และยุโรป โดยรายชื่อที่ OpenAI เผยแพร่ยังปรากฏบริษัทจากเอเชีย เช่น NTT DATA ของญี่ปุ่น Tata Consultancy Services ของอินเดีย และ Axiata Group ของมาเลเซีย ทั้งนี้ การร่วมลงนามเป็นการแสดงเจตนารมณ์ในนามบริษัท มิใช่การลงนามในนามรัฐบาลของประเทศเหล่านั้น

สำหรับประเทศไทย แนวทางที่จดหมายเปิดผนึกเสนอมีความสอดคล้องกับการคุ้มครองโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งครอบคลุมภารกิจและบริการสำคัญ เช่น การเงินการธนาคาร เทคโนโลยีสารสนเทศและโทรคมนาคม การขนส่งและโลจิสติกส์ พลังงานและสาธารณูปโภค ตลอดจนสาธารณสุข นอกจากนี้ประเทศไทยยังมีความร่วมมือในการนำ AI มาเสริมขีดความสามารถด้านการป้องกันภัยไซเบอร์อยู่แล้ว โดยเมื่อวันที่ 2 เมษายน 2568 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และ Google Cloud ได้ประกาศความร่วมมือเชิงกลยุทธ์ เพื่อประยุกต์ใช้เทคโนโลยี AI การวิเคราะห์ข้อมูล

และข้อมูลข่าวกรองด้านภัยคุกคาม สนับสนุนการเฝ้าระวังและตอบสนองต่อเหตุการณ์ที่อาจส่งผลกระทบต่อหน่วยงานภาครัฐและโครงสร้างพื้นฐานสำคัญของประเทศ โดยความร่วมมือดังกล่าวครอบคลุมการแลกเปลี่ยนข้อมูลภัยคุกคาม ตลอดจนการฝึกอบรมเชิงปฏิบัติการด้านการตอบสนองต่อเหตุการณ์นิติวิทยาศาสตร์ดิจิทัลและการวิเคราะห์มัลแวร์ให้แก่บุคลากรภาครัฐที่ได้รับการคัดเลือก นอกจากนี้ ยังมีแผนนำเทคโนโลยีมาใช้ช่วยตรวจสอบเว็บไซต์อันตรายและเว็บไซต์หลอกลวง เพื่อเพิ่มความปลอดภัยให้แก่ประชาชนและผู้ที่อาศัยอยู่ในประเทศไทย

ที่มา:

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, https://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF

สกมช. จับมือ Google Cloud เสริมความมั่นคงไซเบอร์ไทยผ่านความร่วมมือในการป้องกันภัยคุกคามทางไซเบอร์ที่ขับเคลื่อนด้วย AI, https://blog.google/intl/th-th/products/google-for-businesses/google-cloud-ai/

