การมาถึงของ AI Security

จบ

วิชญ์ภูทธ์ เมาะพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา แห่งมหาวิทยาลัยธรรมศาสตร์

ต่อ จากฉบับที่แล้ว

ตัวอย่างการประยุกต์ใช้ AI เพื่อใช้สนับสนุนงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ อาทิ

◆ การสร้างแบบจำลองด้านพฤติกรรมของผู้ใช้งาน

AI จะช่วยสร้างแบบจำลองเพื่อศึกษา และตรวจสอบพฤติกรรมของผู้ใช้งานในระบบขององค์การ เพื่อคัดกรองผู้ใช้งานที่มีประพฤติไม่น่าไว้วางใจ เช่น กรณีมีผู้ใช้งานพยายามแอบลักลอบขโมยข้อมูลการเข้าสู่ระบบของผู้ใช้งานรายอื่นเพื่อนำบัญชีนั้นไปใช้ ก่ออาชญากรรมไซเบอร์ AI จะเรียนรู้พฤติกรรมจากกิจกรรมต่างๆ ที่ผ่านมาในอดีตของผู้ใช้รายนั้น เพื่อจำแนกพฤติกรรมที่ผิดปกติวิสัยมาสร้างเป็นสัญญาณเตือนของการโจมตี และเมื่อถึงตอนนั้น AI จะสามารถโต้ตอบการโจมตีโดยการบล็อคการเข้าถึงระบบของผู้ใช้รายนั้นไว้ชั่วคราวหรือทำการแจ้งเตือนผู้ดูแลระบบเพื่อดำเนินการในขั้นตอนต่อไป เป็นต้น

◆ การนำ AI มาประยุกต์ใช้ในผลิตภัณฑ์ Antivirus

AI Antivirus คือ Antivirus ที่นำเอาความสามารถของ AI มาใช้ในการตรวจจับพฤติกรรมภายในระบบสารสนเทศ และเครือข่ายที่มีเหตุการณ์ผิดปกติต่างๆ โดยทำการวิเคราะห์ และจำแนกพฤติกรรมที่ผิดปกติออกมา เพื่อนำมาวิเคราะห์ว่า เป็นการกระทำจากไวรัสหรือมัลแวร์ หรือไม่ ทำให้เมื่อพบมัลแวร์เข้าสู่เครือข่าย AI Antivirus จะสามารถตรวจจับได้ในทันที ซึ่งต่างจากโปรแกรม Antivirus ในอดีตที่จะใช้วิธีการตรวจสอบพฤติกรรมจากฐานข้อมูล (Virus Definition) ซึ่งหากฐานข้อมูลดังกล่าวไม่ได้มีการ update ให้เป็นข้อมูลปัจจุบันก็อาจทำให้มัลแวร์หลุดรอดเข้าสู่ระบบมาโจมตีได้

◆ การวิเคราะห์เครือข่าย และระบบสารสนเทศแบบอัตโนมัติ

การวิเคราะห์ระบบสารสนเทศหรือระบบเครือข่ายโดยใช้คนวิเคราะห์คงจะเป็นไปได้ค่อนข้างยาก อันเนื่องมาจากปริมาณของข้อมูลกิจกรรมที่เกิดในเครือข่ายมีจำนวนมหาศาล รวมถึงระยะเวลาที่ต้องใช้ในการวิเคราะห์ ซึ่งการทำงานดังกล่าวสามารถนำเอา AI เข้ามาช่วยสนับสนุนได้ เพราะ AI ที่สามารถเปรียบเทียบข้อมูลในเหตุการณ์ปัจจุบันกับข้อมูลเชิงสถิติในอดีตได้ ด้วยวิธีดังกล่าว AI จึงสามารถตรวจจับการบุกรุกเครือข่ายหรือระบบสารสนเทศได้อย่างรวดเร็วกว่าการวิเคราะห์ด้วยผู้เชี่ยวชาญ

◆ การวิเคราะห์ความเสี่ยงจากภัยคุกคามที่แอบแฝงมากับจดหมายอิเล็กทรอนิกส์ (email)

ในปัจจุบัน Hacker ยังคงนิยมใช้ email เป็นเครื่องมือในการโจมตีแบบ Phishing (การลวงเพื่อเข้าถึงข้อมูล) โดยการแนบ link หรือ URLs แปลกปลอมมากับเนื้อหาหรือไฟล์แนบของ email เมื่อถูกเปิดผู้ใช้งานจะถูกล่อลวงให้เข้าใช้หน้าเว็บปลอมหรือการปลอม-แปลงในรูปแบบอื่นๆ ระบบให้บริการ email ที่มี AI จะสามารถทำการตรวจสอบ URLs แปลกปลอมที่แนบมาได้อย่างละเอียด โดยการทดลองคลิกที่ URLs (ใน sandbox) เพื่อวิเคราะห์ความเป็นไปได้ของภัยคุกคาม นอกจากนี้ AI ยังสามารถใช้เทคนิคการตรวจจับความผิดปกติต่างๆ ไม่ว่าจะเป็นในส่วนของผู้ส่ง ตัวเนื้อข้อความ รวมถึงไฟล์แนบ เพื่อนำมาใช้วิเคราะห์ และระบุความเสี่ยง

ตัวอย่างขององค์การชั้นนำที่นำเอา AI มาประยุกต์ใช้งานในด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

➢ PayPal นำ AI มาประยุกต์ใช้จนสามารถลดอัตราการฉ้อโกงให้เหลือเพียง 0.32% ของรายได้โดยใช้ระบบ deep learning เพื่อวิเคราะห์การทำธุรกรรมการเงินแบบ real-time

➢ ระบบรักษาความปลอดภัยของอุปกรณ์ภายในเครือข่ายของ Verizon ใช้ AI ในการบริหารจัดการ และประเมินความเสี่ยง เพื่อช่วยให้องค์การสามารถระบุ และจัดลำดับความสำคัญของความเสี่ยง ทำให้สามารถบริหารจัดการเพื่อรับมือกับภัยคุกคามที่มีความรุนแรงได้ดียิ่งขึ้น

➢ Duke Energy, BP หรือ Honeywell เป็นองค์การชั้นนำในอุตสาหกรรมพลังงานที่มีการประยุกต์ใช้ AI เป็นเครื่องมือวิเคราะห์ข้อมูลจากระบบ real-time sensor เพื่อหลีกเลี่ยงปัญหาหรือเหตุการณ์ไม่พึงประสงค์ที่อาจเกิดขึ้นได้

จากผลสำรวจของสถาบันวิจัย Capgemini องค์การที่ปรึกษาชั้นนำด้าน Technology และ Digital Transformation ที่ทำการสำรวจกลุ่มผู้บริหารจำนวน 850 คนจาก 7 ภาคอุตสาหกรรม อาทิ วงการค้าปลีก ธนาคาร ประกันภัย ยานยนต์ สาธารณูปโภค โทรคมนาคม พบว่า AI นั้นเป็นสิ่งที่จำเป็นในการสร้างความมั่นคงปลอดภัยให้แก่ระบบสารสนเทศ และเครือข่าย โดยมีผลการสำรวจที่สำคัญ อาทิ

➢ 80% ของผู้บริหารในธุรกิจสื่อสารโทรคมนาคม เชื่อว่าองค์การจะไม่สามารถตอบโต้การโจมตี และภัยคุกคามได้โดยปราศจากการสนับสนุนจาก AI

➢ 51% ขององค์การส่วนใหญ่มีการพึ่งพา AI สำหรับการตรวจจับการพยากรณ์ภัยคุกคาม และการตอบโต้การโจมตี

➢ 75% ขององค์การต่างๆ พึ่งพา AI สำหรับการรักษาความปลอดภัยของระบบเครือข่าย

➢ การนำ AI มาใช้ในการรักษาความมั่นคงปลอดภัยมีแนวโน้มที่เพิ่มขึ้น จาก 1 ใน 5 ขององค์การที่ได้ทำการสำรวจใช้ AI มาตั้งแต่ก่อนปี ค.ศ.2019 เป็น 2 ใน 3 ขององค์การที่ได้ทำการสำรวจที่มีการวางแผนจะนำเอา AI มาประยุกต์ใช้ภายในปี ค.ศ. 2020

ภัยคุกคาม และการโจมตีทางไซเบอร์ถูกพัฒนาอย่างต่อเนื่องและมีอัตราที่สูงขึ้นพร้อมกับปัญหาการขาดแคลนบุคลากรผู้เชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัย ทำให้เกิดเป็นข้อแตกต่างที่ชัดเจนของการใช้คนในการวิเคราะห์ภัยคุกคามเมื่อเปรียบเทียบกับความสามารถ และประสิทธิภาพของ AI จนนำไปสู่ความท้าทายในด้านการรักษาความมั่นคงปลอดภัยที่เพิ่มมากขึ้น ซึ่งกลายเป็นว่าเทคโนโลยี AI จะเป็นตัวกระตุ้นให้เกิดการยกระดับความเข้มข้นในการป้องกัน และโจมตีทางไซเบอร์ ระหว่างผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางสารสนเทศ และ Hacker

สำหรับองค์การก็จำเป็นต้องเริ่มศึกษาแนวทางการประยุกต์ใช้งาน AI ในด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศเป็นการเตรียมพร้อมรับมือกับภัยคุกคามรูปแบบใหม่ๆ ที่ทวีความรุนแรงมากขึ้นตามความสามารถของเทคโนโลยี เพื่อให้องค์การสามารถดำเนินงานได้อย่างต่อเนื่อง มีความมั่นคงปลอดภัยต่อองค์การ และผู้ที่เกี่ยวข้องเป็นสำคัญ TPA news

ข้อมูลอ้างอิง

- AI Superpowers, Dr.Kai-Fu Lee
- Why ai is the future of cybersecurity, www.forbes.com
- Artificial intelligence and cybersecurity, www.infosecurity-magazine.com
- Hackers using ai, www.cisomag.com
- hosteddocs.ittoolbox.com/ai_cybersecurity_dummies.pdf
- Leading ai cybersecurity companies, www.comparitech.com
- AI in cybersecurity report, www.capgemini.com