สรุปบทเรียนจากการพัฒนาความรู้

รอบการประเมินที่ 2

ปีงบประมาณ พ.ศ. 2569

หลักสูตร

วิชา Security Foundation for AI: เตรียมความพร้อมด้านความมั่นคงปลอดภัย เพื่อก้าวสู่ AI Ready Organization (รุ่นที่ 1)

จัดทำโดย นายชัยภัทร ป้องที

ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ

การอบรมหลักสูตร Security Foundation for AI: เตรียมความพร้อมด้านความมั่นคงปลอดภัย เพื่อก้าวสู่ AI Ready Organization (รุ่นที่ 1) มุ่งเน้นการสร้างความรู้ความเข้าใจเชิงลึกเกี่ยวกับความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นจากการนำเทคโนโลยีปัญญาประดิษฐ์ โดยเฉพาะอย่างยิ่ง Generative AI มาประยุกต์ใช้ภายในองค์กร โดยครอบคลุมการคุ้มครองความปลอดภัยอย่างเป็นระบบในทุกมิติที่เกี่ยวข้อง ไม่ว่าจะเป็นด้านแอปพลิเคชัน บัญชีผู้ใช้งาน ระบบยืนยันตัวตน อุปกรณ์ปลายทาง ระบบเครือข่าย ข้อมูลสำคัญขององค์กร ตลอดจนระบบคลาวด์ การมองภาพรวมความเสี่ยงในลักษณะนี้ช่วยให้ผู้เข้ารับการอบรมสามารถประเมินผลกระทบได้อย่างรอบด้าน โดยไม่จำกัดอยู่เพียงแค่การรักษาความปลอดภัยของตัวแบบจำลองปัญญาประดิษฐ์ (AI Model) เท่านั้น แต่เป็นการปกป้องสถาปัตยกรรมเทคโนโลยีทั้งหมดขององค์กร

นอกจากนี้ หลักสูตรยังส่งเสริมทักษะการวิเคราะห์สถานการณ์ที่อาจก่อให้เกิดช่องโหว่หรือการรั่วไหลของข้อมูลในทางปฏิบัติได้อย่างมีประสิทธิภาพ เช่น การที่บุคลากรนำข้อมูลลับ เอกสารราชการ หรือข้อมูลส่วนบุคคล (PII) ไปป้อนเข้าสู่ระบบ AI โดยไม่ตั้งใจ การถูกผู้ไม่หวังดีแอบอ้างหรือเข้าถึงระบบ AI ผ่านบัญชีผู้ใช้งานที่ถูกขโมย การเชื่อมต่อแอปพลิเคชันหรือส่วนขยาย (Plugins) ที่ไม่ได้รับอนุญาตหรือไม่ปลอดภัย ตลอดจนการรับมือกับการที่ผู้โจมตีนำเทคโนโลยี AI มาใช้เป็นเครื่องมือในการสร้างข้อความ ลิงก์ หรือไฟล์แนบที่มีลักษณะหลอกลวง (Phishing & Social Engineering) ซึ่งมีความแนบเนียนสูง เพื่อมุ่งเป้าโจมตีบุคลากรภายในองค์กร

ในส่วนของการป้องกันและลดความเสี่ยง ผู้เข้าร่วมการอบรมจะได้เรียนรู้แนวทางการรักษาความปลอดภัยให้กับระบบ AI โดยใช้เครื่องมือมาตรฐานระดับสากลของ Microsoft ซึ่งครอบคลุมการคุ้มครองในหลายมิติ ได้แก่ Microsoft Defender ที่ใช้สำหรับตรวจจับภัยคุกคามเชิงรุก วิเคราะห์พฤติกรรมที่ผิดปกติของผู้ใช้งานและระบบ พร้อมทั้งตรวจสอบเส้นทางที่ผู้โจมตีอาจใช้เป็นช่องทางเข้าถึงบัญชีผู้ใช้ อุปกรณ์ ระบบงาน หรือข้อมูลสำคัญขององค์กร; Microsoft Purview ที่ช่วยในการค้นหา จำแนกประเภท และกำกับดูแลข้อมูลที่มีความละเอียดอ่อน เช่น ข้อมูลส่วนบุคคล ข้อมูลสุขภาพ เอกสารราชการ และข้อมูลความลับภายใน พร้อมทั้งการกำหนดนโยบาย

ป้องกันข้อมูลรั่วไหล (Data Loss Prevention: DLP) จากการใช้งาน AI Microsoft Entra สำหรับบริหารจัดการตัวตนและควบคุมสิทธิ์การเข้าถึงระบบตามแนวคิด Zero Trust เช่น การเปิดใช้งานการยืนยันตัวตนหลายปัจจัย (MFA) การกำหนดเงื่อนไขการเข้าใช้งาน (Conditional Access) และการควบคุมสิทธิ์ของผู้ใช้งานตามบทบาทและระดับความสำคัญของข้อมูล (RBAC) และ Microsoft Intune สำหรับกำกับดูแลและควบคุมความปลอดภัยของอุปกรณ์ปลายทางที่ใช้เข้าถึงระบบ AI ไม่ว่าจะเป็นคอมพิวเตอร์ โทรศัพท์มือถือ หรืออุปกรณ์พกพาอื่น ๆ เพื่อให้มั่นใจว่าอุปกรณ์เหล่านั้นมีความปลอดภัย ปราศจากช่องโหว่ และเป็นไปตามนโยบายขององค์กรก่อนที่จะได้รับอนุญาตให้เข้าถึงข้อมูลหรือระบบงานสำคัญ

ข้อสรุปและแนวคิดในการประยุกต์ใช้เพื่อพัฒนาองค์การ

โดยสรุปแล้ว หลักสูตรนี้จะช่วยให้ผู้เข้าร่วมการอบรมมีความรู้และความเข้าใจในการวางแนวทางการรักษาความปลอดภัยสำหรับการนำ AI มาประยุกต์ใช้ในองค์กรได้อย่างครบวงจร ครอบคลุมทั้งด้านตัวตนผู้ใช้งาน อุปกรณ์ แอปพลิเคชัน เครือข่าย ข้อมูล และระบบคลาวด์ ตลอดจนสามารถนำความรู้และประสบการณ์ที่ได้รับไปประยุกต์ใช้จริงในการกำหนดนโยบายการกำกับดูแล AI (AI Governance) การประเมินและบริหารจัดการความเสี่ยง รวมถึงการยกระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร

แหล่งที่มา

หลักสูตร : Security Foundation for AI: เตรียมความพร้อมด้านความมั่นคงปลอดภัย เพื่อก้าวสู่ AI Ready Organization (รุ่นที่ 1)

ด้านการพัฒนา (ระบุ ✓) : ☑ ดิจิทัล

☐ ความรู้เฉพาะด้านเพื่อใช้ในการปฏิบัติงาน

☑ เพิ่มศักยภาพตนเอง/ประสิทธิภาพในการทำงาน

บรรยายโดย : บริษัท ไมโครซอฟท์ (ประเทศไทย) จำกัด

หน่วยงานผู้รับผิดชอบ : กรมพัฒนาที่ดิน

วิธีการพัฒนาตนเอง : เข้ารับการฝึกอบรม บริษัท ไมโครซอฟท์ (ประเทศไทย) จำกัด

วันที่ได้รับการฝึกอบรม : 29 เมษายน 2569 **สถานที่ :** บริษัท ไมโครซอฟท์ (ประเทศไทย) จำกัด