แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการกลุ่มวางแผนการใช้ที่ดิน

ด้วย นางสาวนิรมล เกษณา ตำแหน่ง นักวิชาการเกษตรชำนาญการพิศษ สังกัด กลุ่มวางแผนการใช้ที่ดิน สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้เพื่อการพัฒนาทักษะด้านดิจิทัลสำหรับบุคลากรภาครัฐ (TDGA E-learning) หลักสูตร Basic Cybersecurity Series: หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น เมื่อวันที่ ๒ กุมภาพันธ์ ๒๕๖๙ เป็นเวลารวมทั้งสิ้น ๑ ชั่วโมง ๓๓ นาที ซึ่งหลักสูตรดังกล่าวจัดโดย สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

จึงขอรายงานสรุปผลการพัฒนาความรู้เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ ดังนี้

๑. วัตถุประสงค์ เพื่อตระหนักและทราบถึงวิธีการป้องกัน (Cybersecurity) และให้ผู้เรียนเข้าใจความหมาย และให้ผู้เรียนเห็นถึงความสำคัญของการประยุกต์ใช้งาน (Cybersecurity) โดยหลักสูตรเป็นช่องทางการสร้างการเรียนรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ (cybersecurity) ระดับต้น (Beginner) จนถึงระดับกลาง (Intermediate) โดยหลักสูตรนี้เหมาะกับผู้ที่สนใจ เจ้าหน้าที่รัฐ พนักงานรัฐ พนักงานเอกชน ที่ต้องการดูแลรักษาและการป้องกัน ธำรงไว้ซึ่ง การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความสมบูรณ์พร้อมใช้ (Availability) เพื่อให้ระบบ/บริการ/ผลิตภัณฑ์ มีความมั่นคงปลอดภัยและสามารถป้องกัน รับมือ ภัยคุกคามที่เกิดจากความมั่นคงปลอดภัยทางไซเบอร์ หรือเหตุการณ์ที่ไม่พึงประสงค์ หรือโอกาสที่จะทำให้เกิดข้อผิดพลาด การสูญเสีย ที่จะเกิดขึ้นต่อระบบ/บริการ/ผลิตภัณฑ์

๒. เนื้อหาและหัวข้อวิชา

เนื้อหาแบ่งออกเป็น ๖ หัวข้อ คือ

๒.๑ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment) คือกระบวนของระบบในการระบุ วิเคราะห์ และจัดลำดับความสำคัญของภัยคุกคาม หรือช่องโหว่ที่อาจส่งผลกระทบต่อสินทรัพย์ดิจิทัลและธุรกิจ ขั้นตอนสำคัญ ได้แก่ การระบุสินทรัพย์, การหาภัยคุกคาม/ช่องโหว่, การประเมินโอกาสและผลกระทบ, การกำหนดมาตรการควบคุมเพื่อลดความเสี่ยง

ขั้นตอนการประเมินความเสี่ยงด้านไซเบอร์

- การเตรียมข้อมูล (Preparation): รวบรวมข้อมูลสินทรัพย์ (Assets) ที่สำคัญ ข้อมูลระบบ, ข้อมูลสารสนเทศ และบุคลากรที่เกี่ยวข้อง
- ระบุความเสี่ยง (Identification): ค้นหาช่องโหว่ (Vulnerabilities) และภัยคุกคาม (Threats) เช่น การแฮก, ไวรัส หรือพนักงานทำข้อมูลรั่วไหล
- วิเคราะห์ความเสี่ยง (Analysis): ประเมินความเป็นไปได้ (Likelihood) และผลกระทบ (Impact) ที่จะเกิดขึ้นหากเกิดเหตุการณ์นั้น
- ประเมินค่าความเสี่ยง (Evaluation): จัดลำดับความสำคัญของความเสี่ยง (เช่น สูง, กลาง, ต่ำ) เพื่อพิจารณาว่าต้องจัดการเร่งด่วนหรือไม่
- จัดการความเสี่ยง (Treatment): กำหนดมาตรการควบคุม, ป้องกัน หรือโอนย้ายความเสี่ยง (เช่น การใช้ Firewall, การทำ Backup, นโยบายรักษาความปลอดภัย)

- ติดตามและทบทวน (Monitoring & Review): ทบทวนความเสี่ยงเป็นระยะเนื่องจากภัยคุกคามเปลี่ยนแปลงตลอดเวลา

ประโยชน์ของการประเมินความเสี่ยง

- ระบุจุดอ่อน: ทำให้ทราบจุดอ่อนในระบบไอทีขององค์กร
- จัดสรรทรัพยากรได้ตรงจุด: ช่วยให้ลงทุนในระบบป้องกันได้คุ้มค่าตามระดับความเสี่ยง
- ปฏิบัติตามกฎหมาย: รองรับการทำมาตรฐาน เช่น ISO ๒๗๐๐๑ หรือกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) องค์กรควรทำการประเมินความเสี่ยงอย่างสม่ำเสมอ เพื่อลดโอกาสเกิดเหตุการณ์โจมตีทางไซเบอร์ที่ส่งผลให้เกิดความเสียหายทั้งข้อมูลและชื่อเสียงขององค์กร

๒.๒ ความสามารถในการเตรียมตัว และตอบสนองต่อภัยคุกคามทางไซเบอร์ (Cyber Resilience) คือ ความสามารถในการป้องกัน ตรวจจับ รับมือ และฟื้นฟูระบบให้กลับมาทำงานได้ตามปกติอย่างรวดเร็วเมื่อเกิดการโจมตี โดยเน้นการสร้างความยืดหยุ่นและการทำงานต่อเนื่องของธุรกิจ (Business Continuity) ผ่านการจัดการความเสี่ยงเชิงรุก การฝึกซ้อมแผนเผชิญเหตุ และการบริหารจัดการบุคลากร/เทคโนโลยี

๒.๓ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) คือ แนวทางเชิงกลยุทธ์ที่ใช้บริหารจัดการความเสี่ยงไซเบอร์ โดยนิยมอิงตามมาตรฐานสากล เช่น NIST CSF ซึ่งครอบคลุม ๕+๑ หลักการสำคัญ คือ การธรรมาภิบาล (Govern), ระบุ (Identify), ป้องกัน (Protect), ตรวจจับ (Detect), ตอบสนอง (Respond) และฟื้นฟู (Recover) เพื่อคุ้มครองข้อมูลและระบบสารสนเทศตามหลัก CIA

กรอบมาตรฐานที่สำคัญ (NIST CSF ๒.๐) ประกอบด้วยองค์ประกอบหลักเพื่อให้องค์กรสามารถป้องกันและรับมือภัยคุกคามได้อย่างเป็นระบบ ได้แก่:

- Govern (การกำกับดูแล): กำหนดนโยบายและแนวทางบริหารความเสี่ยง
- Identify (การระบุ): เข้าใจบริบท ทรัพย์สิน และประเมินความเสี่ยง
- Protect (การป้องกัน): มาตรการป้องกัน เช่น Access Control, การสร้างความตระหนักรู้, การรักษาความปลอดภัยทางกายภาพ
- Detect (การตรวจจับ): การเฝ้าระวังภัยคุกคามและการตรวจสอบความผิดปกติ
- Respond (การตอบสนอง): แผนรับมือ และสื่อสารเมื่อเกิดเหตุ (Incident Response)
- Recover (การฟื้นฟู): แผนกู้คืนระบบและรักษาความต่อเนื่องทางธุรกิจ

หลักการพื้นฐาน (CIA Triad)กรอบมาตรฐานส่วนใหญ่ตั้งอยู่บนหลักการสำคัญ ๓ ประการ คือ:

- Confidentiality (การรักษาความลับ): ข้อมูลเข้าถึงได้เฉพาะผู้มีสิทธิ์
- Integrity (ความสมบูรณ์): ข้อมูลถูกต้อง ไม่ถูกแก้ไขโดยมิชอบ
- Availability (ความพร้อมใช้งาน): ระบบ และข้อมูลสามารถใช้งานได้เมื่อต้องการ

ประโยชน์ของการใช้กรอบมาตรฐาน

- บริหารจัดการความเสี่ยง: ช่วยระบุจุดอ่อน และจัดการความเสี่ยงได้อย่างตรงจุด
- สอดคล้องกฎหมาย: ช่วยให้องค์กรปฏิบัติตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- ยกระดับความเชื่อมั่น: สร้างความมั่นใจต่อลูกค้าและคู่ค้า
- ยืดหยุ่น: สามารถปรับใช้ให้เหมาะกับขนาดขององค์กร

๒.๔ การป้องกันความเสี่ยง (Protect) โดยการประเมินช่องโหว่ (Vulnerability Assessment) กระบวนการหลักของการประเมินช่องโหว่ (๔ ขั้นตอน):

- การระบุช่องโหว่ (Vulnerability Identification): ใช้เครื่องมือ VA Scan ค้นหาจุดอ่อน เช่น ซอฟต์แวร์เก่า, ตั้งค่าไม่ปลอดภัย
- การวิเคราะห์ช่องโหว่ (Vulnerability Analysis): วิเคราะห์สาเหตุและผลกระทบของช่องโหว่ที่พบ
- การประเมินความเสี่ยง (Risk Assessment): จัดลำดับความรุนแรง (เช่น ตามคะแนน CVSS) เพื่อดูว่าจุดใดอันตรายที่สุด
- การแก้ไขและป้องกัน (Remediation): วางแผนแก้ไข ปิดช่องโหว่ หรือติดตั้ง Patch เพื่อป้องกันความเสี่ยง

ประโยชน์ของการประเมินช่องโหว่:

- ลดความเสี่ยง (Risk Reduction): ปิดจุดอ่อนก่อนถูกแฮกเกอร์โจมตี
- ความปลอดภัยเชิงรุก (Proactive Security): ตรวจสุขภาพระบบเป็นประจำ
- ปฏิบัติตามมาตรฐาน (Compliance): สอดคล้องกับข้อกำหนด เช่น PCI DSS, PDPA
- ลดค่าใช้จ่าย (Cost Saving): แก้ไขได้ทันท่วงทีประหยัดกว่าการแก้ปัญหาหลังเกิดเหตุ

โดยปกติควรทำการประเมินช่องโหว่อย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงระบบเครือข่ายครั้งใหญ่ เพื่อให้ระบบมีความปลอดภัยสูงสุด

การประเมินช่องโหว่ (Vulnerability Assessment: VA) เป็นกระบวนการเชิงรุก (Protect) เพื่อค้นหา ระบุ และจัดลำดับความสำคัญของจุดอ่อนด้านความปลอดภัยในระบบไอที แอปพลิเคชัน หรือเครือข่าย ผ่านการสแกนด้วยเครื่องมืออัตโนมัติ เพื่อนำไปสู่การแก้ไข (Remediation) ก่อนถูกโจมตีจริง

๒.๕ การตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ คือ กระบวนการตรวจจับ แจ้งเตือน และวิเคราะห์กิจกรรมที่ผิดปกติในเครือข่าย/ระบบอย่างต่อเนื่อง โดยใช้เครื่องมือ เช่น SIEM, Firewall และการตรวจสอบ Log ย้อนหลัง เพื่อป้องกันการโจมตีแบบเรียลไทม์ ควบคู่กับการตั้งค่าความปลอดภัย, อัปเดตแพตช์ซอฟต์แวร์, จำกัดสิทธิ์การใช้งาน และการสำรองข้อมูลอย่างสม่ำเสมอ

แนวทางปฏิบัติในการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

- การเฝ้าระวังและตรวจจับ (Detection & Monitoring):
  - ใช้งานระบบตรวจจับภัยคุกคาม (IDS/IPS) และระบบบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัย (SIEM) เพื่อแจ้งเตือนอัตโนมัติ
  - ตรวจสอบ Log ข้อมูลการเข้าถึงระบบที่สำคัญย้อนหลังอย่างน้อย ๓๐-๙๐ วันเพื่อหาความผิดปกติ
  - ตรวจสอบการใช้งานเครือข่ายและระบบอย่างต่อเนื่อง (Real-time monitoring)
- มาตรการป้องกันและตรวจสอบพื้นฐาน:
  - ติดตั้งและอัปเดตโปรแกรมป้องกันไวรัส (Anti-malware) และแพตช์ความปลอดภัย (Patch management) อย่างสม่ำเสมอ
  - จำกัดสิทธิ์ผู้ใช้งาน (Principle of Least Privilege) และใช้การยืนยันตัวตนหลายชั้น (Multi-Factor Authentication - MFA)
  - สำรองข้อมูล (Backup) ข้อมูลสำคัญ และเก็บรักษาไว้อย่างปลอดภัย

- การจัดการความเสี่ยงและตอบสนอง:
  - ประเมินความเสี่ยงและระบุจุดอ่อน (Vulnerability Assessment) อย่างสม่ำเสมอ
  - จัดทำแผนรับมือเหตุภัยคุกคามทางไซเบอร์ (Incident Response Plan) และมีเจ้าหน้าที่ประสานงานกับ ThaiCERT
  - อบรมให้ความรู้ด้าน Cyber Hygiene แก่พนักงาน เพื่อลดความเสี่ยงจากการถูกหลอกลวง (Phishing)

การตรวจสอบที่มีประสิทธิภาพควรทำอย่างต่อเนื่องและทบทวนกลไกการตรวจจับอย่างน้อยปีละ ๑ ครั้ง

๒.๖ การเผชิญเหตุภัยคุกคามภัยคุกคามทางไซเบอร์ (Respond) และการฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover)

การเผชิญเหตุ (Respond) และการฟื้นฟู (Recover) เป็นขั้นตอนสำคัญภายหลังการตรวจพบภัยคุกคามไซเบอร์ โดยมุ่งเน้นการจำกัดขอบเขตความเสียหาย ปราบปรามภัยคุกคาม และกู้คืนระบบให้กลับมาทำงานปกติโดยเร็วที่สุด ซึ่งประกอบด้วย การหยุดยั้งการโจมตี, การกำจัดภัยคุกคาม, การกู้คืนข้อมูล และการทบทวนปรับปรุงระบบ (After-Action Review)

การเผชิญเหตุภัยคุกคามทางไซเบอร์ (Respond) เน้นที่การรับมืออย่างรวดเร็วเมื่อเกิดเหตุ (Incident Response - IR) ประกอบด้วยขั้นตอนหลัก:

- การวิเคราะห์และระบุตัวตน (Analysis): ตรวจสอบว่าเป็นเหตุการณ์ภัยคุกคามประเภทใดและประเมินผลกระทบ
- จำกัดขอบเขต (Containment): หยุดยั้งการโจมตีไม่ให้แพร่กระจาย เช่น ตัดการเชื่อมต่อระบบที่ติดเชื้อ, ปิดกั้นพอร์ตเครือข่าย
- การกำจัดภัยคุกคาม (Eradication): ลบโค้ดอันตราย, ลบไฟล์ที่ติดเชื้อ, ปิดช่องโหว่ที่คนร้ายใช้
- การรายงาน (Reporting): บันทึกรายงานสถานการณ์ระดับความรุนแรงและแจ้งรายงานตามโครงสร้าง

การฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover) เน้นการกู้คืนระบบให้กลับมาให้บริการได้ปกติ และปรับปรุงให้ปลอดภัยกว่าเดิม ประกอบด้วยขั้นตอนหลัก:

- การกู้คืนระบบ (Restore/Recovery): นำข้อมูลสำรอง (Backup) มาใช้งานใหม่, เปลี่ยนรหัสผ่านทั้งหมด, ติดตั้งระบบใหม่หากจำเป็น
- การทำความต่อเนื่องทางธุรกิจ (BCP): เปิดใช้งานแผนบริหารจัดการความต่อเนื่อง (Business Continuity Plan) เพื่อให้ธุรกิจยังดำเนินการต่อไปได้
- การทบทวนหลังเกิดเหตุ (Post-Incident Review): วิเคราะห์สาเหตุที่แท้จริง (Root Cause Analysis) และจัดทำรายการตรวจสอบเพื่อป้องกันการเกิดซ้ำ (Lessons Learned)
- การสอบสวนและเก็บหลักฐาน (Investigation): เก็บหลักฐานทางดิจิทัล (Forensic) เพื่อใช้ดำเนินคดีตามกฎหมาย

ทั้งนี้ องค์กรควรกำหนดทีมรับมือ (CIRT) และฝึกซ้อมแผนรับมืออย่างน้อยปีละ ๑ ครั้ง

๓. ประโยชน์ที่ได้รับ มีความรู้ความเข้าใจ ทราบถึงวิธีการป้องกัน (Cybersecurity) และรู้ถึงการประยุกต์ใช้งาน (Cybersecurity)

๔. แนวทางการนำความรู้ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน ข้อมูลของหน่วยงานได้รับการดูแลรักษาและการป้องกัน การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความสมบูรณ์พร้อมใช้ (Availability) มีความมั่นคงปลอดภัย และสามารถป้องกัน รับมือ ภัยคุกคามที่เกิดจากความมั่นคงปลอดภัยทางไซเบอร์ หรือเหตุการณ์ที่ไม่พึงประสงค์ หรือโอกาสที่จะทำให้เกิดข้อผิดพลาด การสูญเสีย ที่จะเกิดขึ้นต่อข้อมูลของหน่วยงานได้

๕. ความต้องการการสนับสนุนจากผู้บังคับบัญชา (ถ้ามี) ควรสนับสนุนให้เจ้าหน้าที่มีความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ และมีการฝึกอบรมเจ้าหน้าที่คอมพิวเตอร์ให้ทันต่อเทคนิคการโจมตีของมัลแวร์ต่าง ๆ อย่างสม่ำเสมอ พร้อมทั้งทำแผนรับมือกับภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นได้

(นางสาวนิรมล เกษณา)
นักวิชาการเกษตรชำนาญการพิเศษ

(นางสุพัตรา บุรีรัตน์)
ผู้อำนวยการสำนักงานพัฒนาที่ดินเขต ๘
รักษาการในตำแหน่งผู้อำนวยการกลุ่มวางแผนการใช้ที่ดิน

ภาคผนวก

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ นิรมล เกษณา

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Basic Cybersecurity Series :

หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 3 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล


DGA
DIGITAL GOVERNMENT DEVELOPMENT AGENCY
TDGA
ประกาศนียบัตร
ให้ไว้เพื่อแสดงว่า
คุณ นิรมล เกษณา
ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน
การเปลี่ยนผ่านสู่องค์กรดิจิทัล
จำนวนชั่วโมงการเรียนรู้ 1:00 ชั่วโมง
โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 2 กุมภาพันธ์ 2569
(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล