แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการสถานีพัฒนาที่ดินพิษณุโลก

ด้วย นางสาวกัลยา เพ็ชรถัด ตำแหน่ง เจ้าพนักงานการเกษตรปฏิบัติงาน สังกัด สถานีพัฒนาที่ดินพิษณุโลก สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้เพื่อการพัฒนาทักษะด้านดิจิทัลสำหรับบุคลากรภาครัฐ (TDGA E-learning) หลักสูตร พัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น หมวดหมู่ ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) เมื่อวันที่ ๒ มิถุนายน ๒๕๖๙ เป็นเวลารวมทั้งสิ้น ๑ ชั่วโมง ๓๐ นาที ซึ่งหลักสูตรดังกล่าวจัดโดย สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

จึงขอรายงานสรุปผลการพัฒนาความรู้เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ ดังนี้

๑. วัตถุประสงค์

๑.๑ เพื่อให้ผู้เข้ารับการอบรมตระหนักและทราบถึงวิธีป้องกัน Cybersecurity

๑.๒ เพื่อให้ผู้เข้ารับการอบรมเข้าใจความหมายและความสำคัญของการประยุกต์ใช้งาน Cybersecurity

๒. เนื้อหาและหัวข้อวิชา

ความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น (Basic Cybersecurity) แบ่งออกเป็น ๖ หัวข้อ ดังนี้

๒.๑ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Risk Assessment)

๒.๒ ความสามารถในการเตรียมตัวและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Cyber Resilience)

๒.๓ กรอบมาตราฐานด้านรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework)

๒.๔ การประเมินช่องโหว่ (Vulnerability Assessment)

๒.๕ การตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๒.๖ การเผชิญเหตุภัยคุกคามภัยคุกคามทางไซเบอร์ (Respond) และการฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover)

ความสำคัญของความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ทำความเข้าใจกับการประเมินความเสี่ยง กระบวนการบริหารความเสี่ยง ตามมาตรฐาน COSO ERM กระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยงเหตุการณ์การกระทำใด ๆ ที่อาจให้เกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และส่งผลกระทบหรือสร้างความเสียหายล้มเหลวหรือโอกาสที่จะบรรลุความสำเร็จต่อการบรรลุเป้าหมายและวัตถุประสงค์ ทั้งในระดับองค์กร ระดับหน่วยงานและระดับบุคคลได้

กระบวนการบริหารความเสี่ยง หมายถึง กลวิธีที่เป็นเหตุเป็นผลที่นำมาใช้ในการบ่งชี้ วิเคราะห์ ประเมิน จัดการ ติดตาม และสื่อสารสิ่งที่เกี่ยวข้องกับกิจกรรมหน่วยงาน/ฝ่ายงาน หรือกระบวนการดำเนินงานขององค์กรเพื่อช่วยลดความสูญเสียในการไม่บรรลุเป้าหมายให้เหลือน้อยที่สุดและเพิ่มโอกาสแก่องค์กรมากที่สุด

การประเมินช่องโหว่ (Vulnerability Assessment) คือ กระบวนการที่ใช้ในการตรวจสอบและระบุช่องโหว่ที่มีอยู่ในระบบหรือแอปพลิเคชัน โดยใช้เครื่องมือตรวจสอบช่องโหว่หรือเทคนิคการสแกนเพื่อค้นหาปัญหาด้านความปลอดภัยของกระบวนการนี้ช่วยให้ทราบถึงช่องโหว่ที่เปิดเผยในระบบหรือ

แอปพลิเคชัน จนนำไปสู่วิธีแก้ไขได้อย่างถูกจุดเพื่อความปลอดภัย เพื่อตรวจสอบความปลอดภัยระบบเครือข่าย ค้นหาช่องโหว่ที่ใช้ภายในองค์กร เช่นระบบปฏิบัติการ (OS) ซอฟต์แวร์ อุปกรณ์ Network อุปกรณ์ Security ฯลฯ นับเป็นเรื่องสำคัญที่ใช้ระบุความรุนแรงของช่องโหว่ที่เกิดขึ้นตามการอ้างอิงของ CVE และ CVSS ช่วยในการประเมินระดับความเสี่ยงช่องโหว่ โดยประเมินความรุนแรงของช่องโหว่และความเสี่ยงที่อาจเกิดขึ้นหากไม่แก้ช่องโหว่นั้น ช่วยในการสร้างรายงานที่รวมข้อมูลเกี่ยวกับช่องโหว่ที่พบ และให้คำแนะนำในการแก้ไขรายงานเหล่านี้ช่วยให้ทีมความมั่นคงปลอดภัยทำประเมินและตัดสินใจในการแก้ไขช่องโหว่ได้อย่างมีประสิทธิภาพ ช่วยในการตรวจสอบว่าระบบสอดคล้องกับมาตรฐาน เช่น PCI DSS หรือ HIPAA หากไม่สอดคล้องจะช่วยในการปรับปรุงความปลอดภัยเพื่อเป็นไปตามข้อกำหนด ช่วยในการค้นพบและแก้ไขช่องโหว่และปัญหาความปลอดภัย ในระหว่างการพัฒนาระบบหรือแอปพลิเคชัน อีกทั้งยังช่วยประหยัดเวลาและค่าใช้จ่ายที่เกิดขึ้นในอนาคตหากมีการโจมตีที่ไม่คาดคิดเกิดขึ้น

รูปแบบของ VA Scan

๑) Host Assessment การประเมินความเสี่ยงในส่วนของ Server ที่มีความสำคัญซึ่งอาจจะเป็นเป้าหมายในการโจมตีได้หากไม่ได้รับการทดสอบอย่างเพียงพอ

๒) Network and Wireless Assessment การประเมินความเสี่ยงโดยมีการกำหนด Policy และนำไปปฏิบัติจริงเพื่อป้องกันไม่ให้มีการเข้าถึงโดยไม่ได้รับอนุญาต

๓) Database Assessment การประเมินความเสี่ยงในเรื่องของ Database หรือระบบที่เกี่ยวข้องกับข้อมูล

๔) Application Scans ใช้วิธีการระบุช่องโหว่ทางด้านความปลอดภัยใน Web Application

การตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) คือระบบตรวจจับความผิดปกติพฤติกรรมผู้ใช้งาน/การโจมตีที่เกิดขึ้นกับระบบหรือข้อมูล/แจ้งเตือนหรือประสานงานไปยังผู้ที่เกี่ยวข้องลดความเสียหายที่อาจเกิดขึ้นได้ สามารถลดโอกาส หรือระยะเวลา ของผู้โจมตีที่จะทำการโจมตีระบบได้ กระบวนการการเฝ้าระวังที่ดี สามารถให้ข้อมูลที่เป็นประโยชน์ในกระบวนการตอบสนองต่อเหตุการณ์ และการกู้คืนระบบได้

ขั้นตอนการรับมือภัยคุกคามทางไซเบอร์

๑) การเตรียมการ เช่น การจัดทำแผนรับมือ ภัยคุกคามทางไซเบอร์ การตั้งทีมตอบสนองต่อเหตุการณ์ การฝึกอบรมพนักงานด้านการรับรู้ความปลอดภัยทางไซเบอร์การเตรียมเครื่องมือต่าง ๆ

๒) การระบุภัยคุกคาม ขั้นตอนนี้เกี่ยวข้องกับการตรวจจับเหตุการณ์ด้านความปลอดภัยที่อาจเกิดขึ้น ซึ่งสามารถเกิดขึ้นได้ ผ่านการแจ้งเตือนจากระบบที่ติดตั้งไว้

๓) การควบคุม เป้าหมายในขั้นตอนนี้คือการหยุดการโจมตีและลดความเสียหายให้น้อยที่สุด เช่น การตัดการเชื่อมต่อระบบเครือข่าย

๔) การกำจัด การกำจัดภัยคุกคามที่ตรวจพบ เช่น การลบไฟล์ Malware เป็นต้น

๓. ประโยชน์ที่ได้รับ ได้รับความรู้ เข้าใจความหมายและความสำคัญของการประยุกต์ใช้งาน Cybersecurity การพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นสิ่งจำเป็นในการทำงาน เข้าใจในภัยคุกคาม การประเมินความเสี่ยง การปฏิบัติเมื่อเกิดเหตุ

๔. แนวทางการนำความรู้ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน นำความรู้ที่ได้รับไปปฏิบัติงานด้านไซเบอร์ และสามารถตรวจสอบการทำงานตามการปฏิบัติงานเบื้องต้นได้อย่างถูกต้อง ปลอดภัย การจัดทำแผนรับมือ ช่วยให้องค์กรสามารถป้องกันและตอบสนองต่อภัยไซเบอร์ได้อย่างมีประสิทธิภาพ

๕. ความต้องการการสนับสนุนจากผู้บังคับบัญชา (ถ้ามี) สนับสนุนบุคลากรเข้ารับการฝึกอบรมเกี่ยวกับไซเบอร์ เพื่อการทำงานได้อย่างมีประสิทธิภาพ

(นางสาวกัลยา เพ็ชรถัด)
เจ้าพนักงานการเกษตรปฏิบัติงาน

(นางสาววันเพ็ญ หลวงกว้าง)
ผู้อำนวยการสถานีพัฒนาที่ดินพิษณุโลก