สรุปบทเรียนที่ได้รับจากการพัฒนาความรู้
ผ่านการอบรมด้วยระบบการเรียนออนไลน์
สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA)

ชื่อ-สกุล นายขจิตพงษ์ นามภักดี
กลุ่ม/ฝ่าย สถานีพัฒนาที่ดินนครราชสีมา สำนักงานพัฒนาที่ดินเขต ๓
หลักสูตร พัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น (Basic Cybersecurity Series)
วันที่อบรม ๙ มิถุนายน ๒๕๖๘
วันที่จบหลักสูตร ๙ มิถุนายน ๒๕๖๘

❖ วัตถุประสงค์

๑. เพื่อให้ผู้เรียนได้ตระหนัก และทราบถึงวิธีการป้องกัน (Cybersecurity) ที่มีประโยชน์ต่อการทำงาน
๒. เพื่อให้ผู้เรียนเข้าใจความหมาย และเห็นความสำคัญของการประยุกต์ให้งาน (Cybersecurity) ป้องกัน ธำรงไว้ซึ่งการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความสามบูรณ์พร้อมใช้ (Availability) เพื่อให้ระบบ/บริวาร/ผลิตภัณฑ์มีความมั่นคงปลอดภัย

❖ สรุปบทเรียน

๑. แนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ความปลอดภัยทางไซเบอร์กลายเป็นข้อมูลที่มีความกังวงทำให้หน่วยงานของรัฐให้ความสำคัญ เนื่องจากการให้บริการในปัจจุบันเป็นการให้บริการผ่านอินเตอร์เน็ต ซึ่งการดำเนินการต้องพึ่งพาเทคโนโลยีเป็นอย่างมาก เมื่อเกิดการถูกคุกคามทางด้านการดำเนินงาน การพัฒนาอาจมีความเสี่ยงหรือช่องโหว่ที่เกิดขึ้นกับตัวระบบ กำหนดมาตรการสำคัญและการรับมือ มีการกำหนดให้ดำเนินการที่มีประสิทธิภาพและสามารถฟื้นตัวได้เร็ว ให้มีการดำเนินการที่มีการต่อเนื่องลดการผิดพลาดที่มีในอนาคต ดังนั้นการบูรณาการกรอบมาตรฐานทางด้านความเป็นสากลจึงเป็นตัวช่วยที่หน่วยงานหรือผู้เรียนนำไปประยุกต์ใช้ในการดำเนินงานของหน่วยงานได้ต่อไป ในปัจจุบันหน่วยงานของรัฐในประเทศไทยดำเนินใช้กรอบมาตรฐานสากลค่อนข้างมาก โดยที่นิยมในไทยคือ (NIST) และ (ISO)

๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment)

๒.๑ ทำความเข้าใจกับการประเมินความเสี่ยง

ความเสี่ยงคือเหตุการณ์ การกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย ความล้มเหลว หรือลดโอกาสที่จะบรรลุเป้าหมายและวัตถุประสงค์ ทั้งในระดับองค์กร ระดับหน่วยงาน และระดับบุคคลได้ ความเสี่ยงมี ๓ รูปแบบ ได้แก่ ๑) โอกาสที่เกิดขึ้น ธุรกิจจะเกิดความเสียหาย (Chance of Loss) ๒) ความเป็นไปได้ที่จะเกิดความเสียหายต่อธุรกิจ (Possibility of Loss)

๓) ความไม่แน่นอน ของเหตุการณ์ที่จะเกิดขึ้น (Uncertainty of Event) โดยจะต้องวางแผนเพื่อลดความเสี่ยง และจัดการความเสี่ยงให้บรรลุวัตถุประสงค์ ให้ชีวิตมีคุณภาพและการดำเนินงานให้ราบรื่น

๒.๒ การบริหารความเสี่ยง (Risk Management)

การบริหารความเสี่ยง หมายถึง กลวิธีที่เป็นเหตุเป็นผลที่นำมาใช้ในการบ่งชี้ วิเคราะห์ ประเมิน จัดการ ติดตาม และสื่อสารสิ่งที่เกี่ยวข้องกับกิจกรรม หน่วยงานฝ่ายงาน หรือกระบวนการดำเนินงานขององค์กร เพื่อช่วยลดความสูญเสียในการไม่บรรลุเป้าหมายให้เหลือน้อยที่สุด และเพิ่มโอกาสแก่องค์กรมากที่สุด ความเสี่ยงที่เกิดขึ้นมีหลากหลายอย่าง เช่น การเมือง เศรษฐกิจ โซเชียลมีเดีย รวมทั้งกฎหมายและภัยธรรมชาติ ซึ่งนำไปสู่ความเสี่ยงจากสภาพแวดล้อมที่จะเกิดขึ้น ความเสี่ยงจากสภาพแวดล้อม แบ่งออกเป็น ๒ ประเภทหลักคือ ๑) สภาพแวดล้อมภายนอก ๒) สภาพแวดล้อมภายใน

๒.๓ ความสำคัญของการบริหารความเสี่ยง

๑) เพื่อส่งเสริมให้องค์กรมีการบูรณาการระหว่างการบริหารความเสี่ยงกับการควบคุมภายใน

๒) เพื่อสะท้อนการพัฒนาในด้านการกำกับดูแลที่ดีขององค์กร การกำหนดวัตถุประสงค์และยุทธศาสตร์องค์กรที่ชัดเจน

๓) เพื่อให้ฝ่ายบริหารเกิดความมั่นใจ ว่าการดำเนินงานจะบรรลุวัตถุประสงค์ได้ตามเป้าหมาย

๔) เพื่อเป็นกลไกในการผลักดันให้องค์กร มีแนวทางการบริหารความเสี่ยง

๒.๔ กระบวนการบริหารจัดการความเสี่ยง

๑) กำหนดวัตถุประสงค์

๒) ระบุความเสี่ยง

๓) ประเมินความเสี่ยง

๔) ประเมินมาตรการควบคุม

๕) การจัดการความเสี่ยง

๖) รายงานผล

๗) การติดตามและทบทวน

๒.๕ กระบวนการจัดการความเสี่ยง ตามมาตรฐาน (COSO ERM)

เป็นหน่วยงานที่ได้เผยแพร่วิธีการและกรอบแนวคิดของการควบคุมภายในขององค์กร อย่างเป็นระบบจนกระทั่งเป็นที่รู้จักและมีความนิยม ต่อมา (COSO) ได้กำหนดนิยามและรูปแบบต่างๆ ในการจัดการกับความเสี่ยง โดยได้กำหนดออกมาเป็น (COSO ERM COSO Enterprise Risk Management)

๒.๖ การประเมินความเพียงพอของการควบคุมภายใน

เป็นการวิเคราะห์ภายใต้แนวคิดการบริหารความเสี่ยง ที่ระบุว่าความเสี่ยงต่างๆ หากดำเนินการได้ภายใต้การควบคุมภายในที่เพียงพอ ก็สามารถรับความเสี่ยงนั้นได้

๒.๗ การประเมินความเสี่ยง

เป็นการวัดระดับความรุนแรงของความเสี่ยงว่ามีมากน้อยเพียงใด โดยนำความเสี่ยงที่ได้จากการระบุความเสี่ยงมาทำการประเมินหาค่าระดับความเสี่ยง โดยแบ่งออกเป็น ๒ มิติ แต่ละมิติจะมีคะแนนในการประเมินออกเป็น ๕ ระดับ ประกอบด้วย

๑) โอกาสเกิดขึ้น (Likelihood) ซึ่งประเมินจากความถี่ของการเกิดเหตุการณ์ที่ก่อให้เกิดความสูญเสียหรือโอกาสที่จะเกิดความเสี่ยง โอกาสของสถานการณ์ความเสี่ยง=จุดอ่อนของสินทรัพย์ (D)+การโจมตี (E)+การทำซ้ำ (R)/๓

เกณฑ์ที่ใช้ในการประเมิน	๑ = โอกาสเกิดขึ้นยากที่สุด	๒ = โอกาสเกิดขึ้นยาก	๓ = โอกาสเกิดขึ้นปานกลาง	๔ = โอกาสเกิดขึ้นง่าย	๕ = โอกาสเกิดขึ้นง่ายที่สุด

๒) ผลกระทบ (Impact) ซึ่งประเมินจากความรุนแรงหรือขนาดของความเสียหายเมื่อเหตุการณ์เกิดขึ้น

๓. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Framework)

กรอบการดำเนินงาน (NIST Cybersecurity Framework) เป็นกรอบมาตรฐานที่ได้รับความนิยมอย่างแพร่หลาย โดยมีฟังก์ชั่นหลัก ๕ ประการ

๑) การระบุความเสี่ยง (Identify)

๒) การป้องกันความเสี่ยง (Protect)

๓) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๔) การเผชิญเหตุภัยคุกคามทางไซเบอร์ (Respond)

๕) การฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover)

๔. การป้องกันความเสี่ยง (Protect) โดยการประเมินช่องโหว่ (Vulnerability Assessment)

๔.๑ การป้องกันความเสี่ยงโดยการประเมินช่องโหว่

๑) Vulnerability Assessment (VA) เป็นกระบวนการที่ใช้ในการตรวจสอบและระบุช่องโหว่ที่มีอยู่ในระบบหรือแอปพลิเคชัน โดยเครื่องมือตรวจสอบช่องโหว่และเทคนิคการแสกน เพื่อค้นหาปัญหาด้านความปลอดภัยซึ่งกระบวนการนี้ช่วยให้ทราบถึงช่องโหว่ที่เปิดเผยในระบบหรือแอปพลิเคชัน จนนำไปสู่วิธีการแก้ไขได้อย่างถูกจุดเพื่อเพิ่มความปลอดภัย

๒) Vulnerability Scanning Tool เป็นเครื่องมือเพื่อตรวจสอบความปลอดภัยระบบเครือข่าย ค้นหาช่องโหว่ที่ใช้งานภายในองค์กร เช่น ระบบปฏิบัติการ (OS) ซอฟต์แวร์ อุปกรณ์ Network อุปกรณ์ Security ซึ่งนับเป็นเรื่องสำคัญที่ใช้ระบุระดับความรุนแรงของช่องโหว่ที่เกิดขึ้นตามการอ้างอิงของ CVE และ CVSS

๔.๒ ประโยชน์ของ Vulnerability Assessment

๑) ช่วยในการประเมินระดับความเสี่ยงที่มาจากช่องโหว่

๒) ช่วยในการสร้างรายงานที่รวมข้อมูลเกี่ยวกับช่องโหว่ที่พบเห็น

๓) ช่วยในการตรวจสอบว่าระบบสอดคล้องกับมาตรฐาน

๔) ช่วยในการค้นพบและแก้ไขช่องโหว่และปัญหาความปลอดภัย

๕. การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๕.๑ การเฝ้าระวังภัยคุกคามต้องทำอย่างต่อเนื่องโดยมีวัตถุประสงค์ ดังนี้

๑) ลดความเสียหายที่อาจเกิดขึ้นได้ หรือสามารถจำกัดวงจรของความเสียหายที่เกิดขึ้นได้

๒) สามารถลดโอกาส หรือระยะเวลาของผู้โจมตีที่จะทำการโจมตีระบบได้

๓) กระกวนการการเผ้าระวังที่ดี สามารถให้ข้อมูลที่เป็นประโยชน์ในกระบวนการการตอบสนองต่อเหตุการณ์และการกู้คืนระบบได้

๕.๒ ตัวอย่างเหตุการณ์ผิดปกติ

๑) พบการ Login ที่ผิดพลาดเพื่อพยายามเข้าสู่ระบบเป็นจำนวนมาก

๒) การ Login เข้าสู่ระบบนอกเวลางาน

๓) พบการ Login มากจากต้นทางที่น่าสงสัย เช่น พบการ Login มาจากต่างประเทศ โดยที่หน่วยงานเองไม่มีเจ้าหน้าที่ที่อยู่ประเทศนั้นๆ

๔) การเรียกใช้งาน Program หรือ Library ที่ผิดปกติ

๕) การทำงานของ CPU หรือการใช้งานระบบเครือข่ายมากผิดปกติ

๖) มีการติดต่อไปยัง IP address หรือ Domain ที่ถูกระบุว่าเป็น Malicious

๖. การเผชิญเหตุภัยคุกคามทางไซเบอร์ (Respond) และการฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover)

๖.๑ ขั้นตอนการการรับมือภัยคุกคามทางไซเบอร์

๑) การเตรียมการ

๒) การระบุภัยคุกคาม

๓) การควบคุม

๔) การกำจัด

เมื่อครบทุกขั้นตอนแล้วควรมีการวิเคราะห์สาเหตุของเหตุการณ์ที่เกิดขึ้น และมีการบันทึกเป็นข้อเสนอแนะไปยังหน่วยงานที่เกี่ยวข้องต่อไป เพื่อลดผลกระทบหรือปรับปรุงกระบวนการในอนาคต เพื่อไม่ให้เกิดปัญหาดังกล่าวขึ้นอีก ผู้ที่สนใจสามารถศึกษาได้จากเอกสารของ NIST ทั้งในขั้นตอนรับมือภัยคุกคามหน่วยงานควรมีแผนการสื่อสารในภาวะวิกฤต เพื่อให้ข่าวสารที่เผยแพร่ออกไปในช่วงเกิดเหตุการณ์การโจมตีมีความครบถ้วนและรวดเร็ว เพื่อให้ผู้ที่มีส่วนได้ส่วนเสียจะได้เตรียมตัวรับมือได้ทัน ควรมีการกำหนดช่องทางในการกระจายข่าวให้เหมาะสม และควรกำหนดให้มีโฆษกในกรณีที่จำเป็นต้องให้ข่าวกับสื่อมวลชน

๖.๒ การกู้คืนระบบ

๑) การจัดทำแผนความต่อเนื่องทางธุรกิจ ควรปรับปรุงทบทวนแผนอย่างน้อยปีละ ๑ ครั้ง

๒) การสำรองข้อมูล

๓) ปรับปรุงมาตรการรักษาความปลอดภัย

DIGITAL GOVERNMENT DEVELOPMENT AGENCY

สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
TDGA
THAILAND DIGITAL GOVERNMENT ACADEMY

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ ขจิตพงษ์ นามภักดี

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Basic Cybersecurity Series : หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

รวมระยะเวลาทั้งสิ้น 1 : 30 **ชั่วโมง**

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ไว้ ณ วันที่ 9 มิถุนายน 2568

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2025-06-09T13:00:23.136+07:00
765fae05