แบบรายงานสรุปบทเรียน

ชื่อหลักสูตร : Basic Cybersecurity ความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

วันที่เข้ารับการอบรม : ๑๕ กุมภาพันธ์ ๒๕๖๙

สถานที่ : หลักสูตรออนไลน์ (TDGA e-Learning)

จัดโดย : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy (TDGA)

ผู้จัดทำรายงาน : นางสาวรัตนาภร แสงเย็น ตำแหน่ง นักวิชาการเงินและบัญชีปฏิบัติการ

วัตถุประสงค์

เพื่อให้มีความรู้ความเข้าใจในกระบวนการรักษาความมั่นคงปลอดภัยสารสนเทศ สามารถระบุความเสี่ยง ป้องกัน และรับมือกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับระบบงาน บริการ หรือข้อมูลสำคัญขององค์กรได้อย่างมีประสิทธิภาพ

สรุปเนื้อหาการฝึกอบรม

๑. การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment)

การประเมินความเสี่ยงด้านความปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) คือ กระบวนการระบุและประเมินภัยคุกคามต่อระบบดิจิทัล เพื่อวางแผนป้องกันอย่างมีลำดับความสำคัญ โดยมีองค์ประกอบหลักดังนี้

- Asset: สินทรัพย์ที่ต้องปกป้อง (ข้อมูล, เซิร์ฟเวอร์)
- Threat: ภัยคุกคาม (Hacker, Malware, ความผิดพลาดของพนักงาน)
- Vulnerability: ช่องโหว่ของระบบ (Software ไม่อัปเดต)
- Impact: ผลกระทบหากเกิดเหตุ (เสียชื่อเสียง, ค่าปรับทางกฎหมาย, ธุรกิจหยุดชะงัก)

๑.๑ การออกแบบระบบรักษาความปลอดภัย มักอ้างอิงโมเดลพื้นฐาน Security Models หรือ CIA ประกอบด้วยหลักการพื้นฐาน ๓ ประการ

- Confidentiality: การรักษาความลับ (เฉพาะผู้มีสิทธิ์เท่านั้นที่เข้าถึงได้)
- Integrity: ความถูกต้องครบถ้วน (ข้อมูลไม่ถูกแก้ไขโดยพลการ)
- Availability: ความพร้อมใช้งาน (ระบบต้องใช้งานได้เมื่อต้องการ)

๑.๒ กรอบมาตรฐานสากลด้านความมั่นคงปลอดภัยทางไซเบอร์ที่นิยมใช้ในประเทศ องค์กรส่วนใหญ่มักประยุกต์ใช้ ๒ มาตรฐานนี้ร่วมกัน คือ

- NIST Cybersecurity Framework (CSF) ๒.๐ (National Institute of Standards and Technology) เน้นความยืดหยุ่นและการจัดการความเสี่ยงเชิงปฏิบัติ
- ISO/IEC (International Organization for Standardization) เป็นมาตรฐานสากล ด้าน Information Security Management System (ISMS) ที่เน้นการบริหารจัดการทั้งองค์กร

๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๑ ความหมายของความเสี่ยง (Definition of Risk)

ความเสี่ยง (Risk) คือ เหตุการณ์ การกระทำใด ๆ ที่อาจขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน หรือผลกระทบของ "ความไม่แน่นอน" ที่มีต่อวัตถุประสงค์หรือเป้าหมายขององค์กร หากพูดในเชิงไซเบอร์ คือโอกาสที่ภัยคุกคาม (Threat) จะอาศัยช่องโหว่ (Vulnerability) ของระบบเพื่อสร้างความเสียหายต่อสินทรัพย์สารสนเทศ แบ่งเป็น ๓ องค์ประกอบหลัก เพื่อให้เห็นภาพรวมของความเสียหายที่อาจเกิดขึ้น ดังนี้

๑) โอกาสที่จะเกิดขึ้น (Likelihood / Probability) คือ การประเมินว่าเหตุการณ์ไม่พึงประสงค์นั้นมี "ความถี่" หรือ "ความเป็นไปได้" มากน้อยเพียงใดที่จะเกิดขึ้นในช่วงเวลาที่กำหนด

๒) ความเป็นไปได้ที่จะเกิดความเสียหายของธุรกิจ (Business Impact) คือ การประเมิน "ระดับความรุนแรง" หรือผลกระทบที่จะเกิดขึ้นต่อองค์กรหากเหตุการณ์นั้นเกิดขึ้นจริง โดยพิจารณาตามหลัก CIA (ความลับ, ความถูกต้อง, ความพร้อมใช้)

๓) ความไม่แน่นอนของเหตุการณ์ที่จะเกิดขึ้น (Uncertainty of Event) คือ สภาวะของการ "ขาดความรู้" หรือข้อมูลที่ชัดเจนเกี่ยวกับเหตุการณ์ในอนาคต ทำให้ไม่สามารถทำนายผลลัพธ์ได้อย่างแม่นยำ ๑๐๐%

การบริหารความเสี่ยง (Risk Management)

การบริหารความเสี่ยง คือ กระบวนการที่เป็นระบบในการระบุ วิเคราะห์ ประเมิน และจัดการกับความเสี่ยงให้อยู่ในระดับที่องค์กร ยอมรับได้ (Risk Appetite) โดยมีกระบวนการตัดสินใจเลือกวิธีรับมือ (Risk Treatment) ที่เหมาะสมที่สุด เพื่อรักษาความต่อเนื่องของธุรกิจ (Business Continuity) และสร้างความมั่นใจให้กับผู้มีส่วนได้ส่วนเสีย

การวิเคราะห์สภาพแวดล้อม (Environment Analysis) เป็นขั้นตอนสำคัญในการประเมินความเสี่ยง เพราะช่วยให้เราเห็นที่มาของภัยคุกคามและจุดอ่อนภายในองค์กร แบ่งเป็น

๑) สภาพแวดล้อมภายนอก ได้แก่
   - ปัจจัยด้านสังคม (Socio-cultural Factors) คือการเปลี่ยนแปลงในพฤติกรรมและการดำเนินชีวิตของผู้คนในสังคม
   - ปัจจัยด้านเศรษฐกิจ (Economic Factors) คือสภาพเศรษฐกิจที่ส่งผลต่อแรงจูงใจในการโจมตีและการลงทุนด้านความปลอดภัย
   - ปัจจัยด้านการเมืองและกฎหมาย (Political and Legal Factors) คือข้อกำหนดทางกฎหมายและสถานการณ์ความขัดแย้งระดับประเทศ
   - ปัจจัยด้านกายภาพ (Physical Factors) คือสภาพแวดล้อมทางธรรมชาติและสถานที่ตั้งที่ส่งผลต่อระบบไอที
   - ปัจจัยด้านเทคโนโลยี (Technological Factors) คือการอุบัติขึ้นของนวัตกรรมใหม่ที่สร้างทั้งโอกาสและภัยคุกคาม

๒) สภาพแวดล้อมภายใน ได้แก่
   - Structure and Policy (โครงสร้างและนโยบาย) การจัดวางโครงสร้างองค์กรที่เอื้อต่อความปลอดภัยไซเบอร์ และการกำหนดนโยบาย (Policy) เพื่อเป็นแนวทางปฏิบัติ

- Service (การบริการและระบบงาน) รูปแบบการให้บริการขององค์กร
- Manpower (บุคลากร) จำนวนและทักษะความสามารถของพนักงาน รวมถึงความตระหนักรู้ด้านไซเบอร์
- Money (งบประมาณ) การจัดสรรงบประมาณสำหรับการจัดซื้อเทคโนโลยี การบำรุงรักษา และการพัฒนาบุคลากร
- Materials (อุปกรณ์และเครื่องมือ) ทรัพยากรทางกายภาพ เช่น ฮาร์ดแวร์, ซอฟต์แวร์, อุปกรณ์เครือข่าย และระบบจัดเก็บข้อมูล (Data Center)
- Management (การบริหารจัดการ) วิสัยทัศน์และการสนับสนุนจากผู้บริหาร รวมถึงกระบวนการตัดสินใจและการรับมือกับวิกฤต

๒.๒ การบริหารความเสี่ยงองค์กรตามกรอบของ COSO ERM (Enterprise Risk Management)

เป็นมาตรฐานสากลที่ช่วยให้องค์กรจัดการกับความไม่แน่นอน เพื่อเพิ่มโอกาสในการบรรลุเป้าหมายและสร้างมูลค่าเพิ่ม (Value) ให้กับผู้มีส่วนได้ส่วนเสีย ปัจจุบัน COSO ERM มีการอัปเดตเป็นฉบับปี ๒๐๑๗ (Integrating with Strategy and Performance) ซึ่งเน้นการเชื่อมโยงความเสี่ยงเข้ากับ "กลยุทธ์" และ "ผลการดำเนินงาน" โดยแบ่งออกเป็น ๕ องค์ประกอบหลัก

๑) การกำกับดูแลและวัฒนธรรมองค์กร (Governance and Culture) คณะกรรมการต้องสอดส่องดูแลความเสี่ยงอย่างจริงจัง สร้างความตระหนักรู้เรื่องความเสี่ยงให้เป็นส่วนหนึ่งของพนักงาน กำหนดจริยธรรม และค่านิยมหลักที่ชัดเจน

๒) กลยุทธ์และการกำหนดวัตถุประสงค์ (Strategy and Objective-Setting) ความเสี่ยงไม่ได้เกิดขึ้นแยกจากกลยุทธ์ แต่ต้องพิจารณาไปพร้อมกัน เข้าใจสภาพแวดล้อมทางธุรกิจ องค์กรต้องรู้ว่าตนเองยอมรับความเสียหายได้แค่ไหนเพื่อแลกกับผลตอบแทน ประเมินว่ากลยุทธ์ที่เลือกมีความเสี่ยงอะไรแฝงอยู่บ้าง

๓) ผลการดำเนินงาน (Performance) คือขั้นตอนการจัดการความเสี่ยงที่เกิดขึ้นจริงในทางปฏิบัติ มองหาเหตุการณ์ที่อาจกระทบต่อเป้าหมาย วิเคราะห์ "โอกาสที่เกิด" และ "ผลกระทบ" (Likelihood & Impact) เลือกวิธีจัดการ เช่น ยอมรับ (Accept), หลีกเลี่ยง (Avoid), ลด (Reduce) หรือ แบ่งปัน (Share)

๔) การทบทวนและปรับปรุง (Review and Revision) ความเสี่ยงเดิมอาจหายไปและความเสี่ยงใหม่จะเข้ามา ดูว่าปัจจัยภายนอก/ภายในเปลี่ยนไปอย่างไร วิธีจัดการความเสี่ยงที่ทำไปนั้นได้ผลจริงหรือไม่ และพัฒนากระบวนการบริหารความเสี่ยงให้มีประสิทธิภาพยิ่งขึ้น

๕) ข้อมูล การสื่อสาร และการรายงาน (Information, Communication, and Reporting) คือการทำให้ข้อมูลไหลเวียนไปทั่วองค์กร ใช้เทคโนโลยีเข้ามาช่วยจัดเก็บและวิเคราะห์ข้อมูลความเสี่ยง สื่อสารทั้งจากบนลงล่าง (Top-down) และล่างขึ้นบน (Bottom-up) รายงานสถานะความเสี่ยงต่อผู้บริหารและคณะกรรมการอย่างสม่ำเสมอ

๒.๓ กระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑) การระบุบริบทและทรัพย์สินสารสนเทศ (Asset Identification) สำรวจต้นทุนที่มี เพื่อกำหนดขอบเขตของการป้องกัน

- การสำรวจทรัพย์สิน ระบุรายการ Hardware, Software, Data และ Network ทั้งหมด
- การจัดชั้นความลับ จำแนกความสำคัญของข้อมูล (เช่น ข้อมูลสาธารณะ, ข้อมูลภายใน, ข้อมูลลับเฉพาะ)
- การระบุเจ้าของสินทรัพย์ กำหนดผู้รับผิดชอบ (Asset Owner) เพื่อให้การจัดการชัดเจน

๒) การระบุและวิเคราะห์ภัยคุกคาม (Threat & Vulnerability Analysis) เป็นการมองหา "ช่องโหว่" และ "อันตราย" ที่อาจเกิดขึ้น

- ภัยคุกคาม (Threats): เช่น แฮกเกอร์, มัลแวร์เรียกค่าไถ่ (Ransomware), ภัยธรรมชาติ หรือความประมาทของพนักงาน
- ช่องโหว่ (Vulnerabilities): เช่น ซอฟต์แวร์ที่ไม่อัปเดต, รหัสผ่านที่คาดเดาง่าย, หรือการขาดนโยบายควบคุมการเข้าถึง
- การประเมินโอกาสและผลกระทบ ใช้สูตร Risk = Likelihood x Impact เพื่อคำนวณระดับความเสี่ยง (Risk Score)

๓) การประเมินและจัดลำดับความเสี่ยง (Risk Evaluation & Prioritization) นำผลวิเคราะห์มาเทียบกับ "เกณฑ์ที่ยอมรับได้" (Risk Appetite) ขององค์กร

- Risk Matrix สรุปความเสี่ยงลงในตารางความร้อน (Heat Map) เพื่อแยกแยะระดับความรุนแรง
- ลำดับความสำคัญ คัดเลือกความเสี่ยงที่มีนัยสำคัญ (เช่น ระดับสูง-สูงมาก) มาจัดทำแผนจัดการก่อน เพื่อให้คุ้มค่ากับงบประมาณและทรัพยากรที่มีจำกัด

๔) การเลือกมาตรการจัดการความเสี่ยง (Risk Treatment Plan) ตัดสินใจว่าจะจัดการความเสี่ยงแต่ละข้ออย่างไร

- Reduce (ลด): ติดตั้ง Firewall, ทำระบบสำรองข้อมูล (Backup), ฝึกอบรมพนักงาน (Phishing Awareness)
- Transfer (โอน): การซื้อประกันภัยไซเบอร์ (Cyber Insurance) หรือใช้บริการ Managed Security Services
- Avoid (เลี่ยง): ยกเลิกการใช้งานระบบที่ล้าสมัยและเสี่ยงเกินไป
- Accept (ยอมรับ): ยอมรับความเสี่ยงในระดับที่ต่ำมากและไม่คุ้มค่าที่จะลงทุนป้องกันเพิ่ม

๕) การติดตามผลและการสื่อสาร (Monitoring & Reporting) ไซเบอร์เป็นเรื่องที่ไม่นิ่ง จึงต้องมีการตรวจสอบอย่างต่อเนื่อง

- การตรวจสอบสม่ำเสมอ ประเมินความเสี่ยงซ้ำอย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนระบบใหม่
- การรายงานเหตุการณ์ (Incident Reporting) บันทึกสถิติการถูกโจมตีและประสิทธิภาพของมาตรการที่ใช้
- การปรับปรุงอย่างต่อเนื่อง นำบทเรียนจากเหตุการณ์จริงมาปรับปรุงแผนป้องกันให้ทันสมัย

๓. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework)

๓.๑ NIST Cybersecurity Framework (CSF) เปรียบเสมือนพิมพ์เขียวระดับสากลที่ช่วยให้องค์กรบริหารจัดการความเสี่ยงทางไซเบอร์ได้อย่างเป็นระบบ โดยจุดเด่นคือการใช้ภาษาที่เข้าใจง่ายทั้งในมุมเทคนิคและมุมบริหารจัดการ ปัจจุบัน NIST CSF ได้พัฒนาจากเวอร์ชั่น ๑.๑ เป็น เวอร์ชั่น ๒.๐ แล้ว โดยมีโครงสร้างหลักที่เรียกว่า Core Functions ซึ่งครอบคลุมวงจรชีวิตของการจัดการความมั่นคงปลอดภัย ดังนี้

- Govern (กำกับดูแล): กำหนดกลยุทธ์ บทบาท และนโยบาย เพื่อให้แน่ใจว่าองค์กรเข้าใจความเสี่ยงและมีทิศทางที่ชัดเจน
- Identify (ระบุ): ทำความเข้าใจสินทรัพย์, ระบบ, ข้อมูล และความเสี่ยงทางธุรกิจขององค์กร
- Protect (ป้องกัน): มาตรการควบคุมที่ออกแบบมาเพื่อปกป้องสินทรัพย์ (เช่น การควบคุมการเข้าถึง, การฝึกอบรมพนักงาน)
- Detect (ตรวจจับ): การเฝ้าระวังและตรวจหาเหตุการณ์ผิดปกติอย่างทันท่วงที
- Respond (ตอบสนอง): ขั้นตอนการดำเนินการเมื่อเกิดภัยคุกคาม เพื่อลดผลกระทบ
- Recover (กู้คืน): การฟื้นฟูระบบและบริการให้กลับมาทำงานได้ปกติหลังเกิดเหตุ

แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานอ้างอิงตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพื่อเป็นมาตรฐานขั้นต่ำที่หน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure - CII) ต้องปฏิบัติ โดยมีวัตถุประสงค์เพื่อสร้างมาตรฐานการปฏิบัติงานให้เป็นไปในทิศทางเดียวกัน ลดช่องโหว่ของโครงสร้างพื้นฐานที่สำคัญของประเทศ

NIST CSF คือเครื่องมือและกรอบแนวทาง (Framework) ในการปฏิบัติ เพื่อให้บรรลุตามข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ ที่แนวทางปฏิบัติฯ พ.ศ. ๒๕๖๔ ของไทยกำหนดไว้เป็นมาตรฐานขั้นต่ำ

การเปลี่ยนแปลงที่สำคัญในเวอร์ชัน ๒.๐ มีการเพิ่ม Govern เข้ามาเป็นศูนย์กลางของทุกฟังก์ชัน โดยมีวัตถุประสงค์เพื่อ

- สร้างธรรมาภิบาล: กำหนดบทบาท ความรับผิดชอบ และนโยบายจากระดับบนลงล่าง (Top-down)
- บริหารความเสี่ยง: ทำให้การรักษาความปลอดภัยไซเบอร์เป็นเรื่องเดียวกับความเสี่ยงทางธุรกิจ ไม่ใช่แค่เรื่องของฝ่าย IT
- การสื่อสาร: ช่วยให้ CISO สามารถสื่อสารงบประมาณและความเสี่ยงกับบอร์ดบริหาร (Board of Directors) ได้เข้าใจง่ายขึ้น

ความแตกต่างของโครงสร้าง

- V ๑.๑: มี ๕ Functions, ๒๓ Categories, ๑๐๘ Subcategories
- V ๒.๐: มี ๖ Functions, ๒๒ Categories, ๑๐๖ Subcategories (มีการปรับลดความซ้ำซ้อนและจัดกลุ่มใหม่ให้กระชับขึ้น)

๔. การป้องกันความเสี่ยง (Protect) โดยการประเมินช่องโหว่ (Vulnerability Assessment (VA))

คือ กระบวนการที่ใช้ในการตรวจสอบและระบุช่องโหว่ที่มีอยู่ในระบบ หรือแอปพลิเคชัน โดยใช้เครื่องมือตรวจสอบช่องโหว่และเทคนิคการสแกนเพื่อค้นหาปัญหาด้านความปลอดภัย ซึ่งกระบวนการนี้ช่วยให้ทราบถึงช่องโหว่ที่เปิดเผยในระบบหรือแอปพลิเคชันจนนำไปสู่การแก้ไขได้อย่างถูกจุดเพื่อเพิ่มความปลอดภัย โดยใช้เครื่องมือเพื่อตรวจสอบความปลอดภัยระบบเครือข่ายค้นหาช่องโหว่ที่ใช้งานภายในองค์กร เช่น ระบบปฏิบัติการ

๔.๑ รูปแบบของ VA Scan

๑) Host Assessment การประเมินความเสี่ยงในส่วนของ Server ที่มีความสำคัญ ซึ่งอาจจะเป็นเป้าหมายในการโจมตีได้หากไม่ได้รับการทดสอบอย่างเพียงพอ

๒) Network and Wireless Assessment การประเมินความเสี่ยงโดยมีการกำหนด Policy และนำไปปฏิบัติจริงเพื่อป้องกันไม่ให้มีการเข้าถึงโดยไม่ได้รับอนุญาต

๓) Database Assessment การประเมินความเสี่ยงในเรื่องของ Database หรือระบบที่เกี่ยวข้องกับข้อมูล

๔) Application Scans ใช้วิธีการระบุช่องโหว่ทางด้านความปลอดภัย Web Application และ Source Code โดยการ Scan แบบอัตโนมัติที่ Front-end หรือไม่ก็วิเคราะห์ที่ Source Code

๔.๒ วงจรการบริหารจัดการช่องโหว่เชิงรุก (Vulnerability Management Lifecycle)

เป็นกระบวนการที่เป็นระบบในการค้นหา วิเคราะห์ ประเมิน และแก้ไขจุดอ่อนของระบบสารสนเทศเพื่อลดโอกาสที่จะถูกโจมตีทางไซเบอร์ ดังนี้

๑) Vulnerability Identification (Testing) การระบุช่องโหว่โดยวิธีการทดสอบจุดประสงค์ คือการเตรียมรายการของช่องโหว่ใน Application ผู้ที่วิเคราะห์จะทำการทดสอบความแข็งแรงของระบบ Security หรือระบบอื่น ๆ โดยใช้เครื่องมือในการ Scan ระบบให้โดยอัตโนมัติ ซึ่งต้องใช้ข้อมูลจากการประกาศของ Vendor ที่มีการเก็บ Vulnerability Database ไว้

๒) Vulnerability Analysis การวิเคราะห์ช่องโหว่และภัยคุกคาม จุดประสงค์คือการหาสาเหตุหรือต้นตอที่เจอช่องโหว่ รวมถึงการระบุรายละเอียดของการทำงานของระบบและสาเหตุของการเกิดช่องโหว่

๓) Risk Assessment การประเมินความเสี่ยง จุดประสงค์คือการจัดลำดับความสำคัญช่องโหว่ จะระบุเป็น Rank หรือ Score ว่าช่องโหว่ไหนร้ายแรงกว่ากัน โดยอ้างอิงจากระบบที่ได้รับผลกระทบข้อมูลอะไรบ้างที่เป็นความเสี่ยงที่ง่ายต่อการโจมตี

๔) Remediation การแก้ไข จุดประสงค์คือ การอุดช่องโหว่ โดยส่วนใหญ่จะเป็นการรวมมือกันระหว่างทีมงานที่ดูแลเรื่อง Security กับทีม Operation ซึ่งเป็นผู้ที่สามารถบอกได้ว่าการอุดช่องโหว่แบบใด ระดับไหนจะมีประสิทธิภาพสูงสุดโดยที่ไม่กระทบระบบปัจจุบัน หรืออาจจะกระทบน้อยลง

๕. การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๕.๑ วัตถุประสงค์

- เพื่อลดความเสียหายที่อาจเกิดขึ้น หรือสามารถจำกัดวงของความเสียหายที่เกิดขึ้นได้
- สามารถลดโอกาส หรือระยะเวลาของผู้โจมตีที่จะทำการโจมตีระบบได้
- กระบวนการเฝ้าระวังที่ดีสามารถให้ข้อมูลที่เป็นประโยชน์ในกระบวนการตอบสนองต่อเหตุการณ์และการกู้คืนระบบได้

๕.๒ รูปแบบของตรวจจับ (Detect Function)

- พบการ Login ที่ผิดพลาด เพื่อพยายามเข้าสู่ระบบเป็นจำนวนมาก
- การ Login เข้าสู่ระบบนอกเวลางาน
- พบการ Login มาจากต้นทางที่น่าสงสัย เช่น พบการ Login จากต่างประเทศโดยที่หน่วยงานไม่มีเจ้าหน้าที่อยู่ประเทศนั้น ๆ
- การเรียกใช้งาน Program หรือ Library ที่ผิดปกติ
- การทำงานของ CPU หรือการใช้งานระบบเครือข่ายมากผิดปกติ
- มีการติดต่อไปยัง IP address หรือ Domain ที่ถูกระบุว่าเป็น Malicious

๖. การเผชิญเหตุภัยคุกคามภัย คุกคามทางไซเบอร์ (Respond) และการฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover)

๖.๑ การเผชิญเหตุภัยคุกคาม (Respond)

เป็นขั้นตอนที่ต้องทำอย่างรวดเร็วเพื่อหยุดยั้งความเสียหาย แบ่งเป็นขั้นตอนย่อยได้ดังนี้

๑) การเตรียมการ (Preparation)
- จัดตั้งทีมตอบโต้เหตุการณ์ (Incident Response Team - IRT) พร้อมระบุบทบาทหน้าที่ชัดเจน
- จัดทำคู่มือ (Playbook) สำหรับภัยคุกคามแต่ละประเภท เช่น Ransomware, Phishing
- เตรียมเครื่องมือสำหรับวิเคราะห์และกู้คืนระบบให้พร้อมใช้งานเสมอ

๒) การระบุภัยคุกคาม (Detection & Analysis)
- ตรวจสอบสัญญาณเตือน (Alerts) จากระบบเฝ้าระวังเพื่อยืนยันว่าเป็นเหตุการณ์จริงหรือไม่
- วิเคราะห์ขอบเขตความเสียหาย (Scope) ว่ากระทบกี่ระบบ ข้อมูลประเภทไหนรั่วไหล
- ระบุประเภทของภัยคุกคามเพื่อเลือกวิธีการรับมือที่เหมาะสม

๓) การควบคุมความเสียหาย (Containment):
- ระยะสั้น แยกเครื่องที่ติดเชื้อออกจากเครือข่าย (Isolate) ทันทีเพื่อไม่ให้มัลแวร์แพร่กระจาย
- ระยะยาว ปรับปรุงกฎ Firewall หรือปิดช่องโหว่ชั่วคราวเพื่อกั้นวงความเสียหาย

๔) การกำจัดภัยคุกคาม (Eradication):
- ลบมัลแวร์ ลบชื่อผู้ใช้งานที่แปลกปลอม หรือล้างเครื่องที่ถูกโจมตี

- ตรวจสอบให้แน่ใจว่าไม่มีประตูหลัง(Backdoor)หลงเหลืออยู่ที่แฮกเกอร์จะกลับมาได้อีก

๖.๒ การฟื้นฟูความเสียหาย (Recover)

การทำให้ระบบกลับมาทำงานตามปกติและสร้างความเชื่อมั่นกลับคืนมา

๑) การกู้คืนระบบ (Recovery)

- กู้คืนข้อมูลจากสำเนาที่ปลอดภัย (Backup) ที่ตรวจสอบแล้วว่าไม่มีมัลแวร์ปนเปื้อน
- เปลี่ยนรหัสผ่านใหม่ทั้งหมด (Global Password Reset) และติดตั้ง Patch ล่าสุด

๒) การทดสอบ (Testing) ตรวจสอบระบบหลังกู้คืนว่าทำงานได้ปกติและไม่มีภัยคุกคามแฝงตัวอยู่

๓) บทเรียนหลังเหตุการณ์ (Post-Incident Activity) ประชุมสรุปปัญหาที่เกิดขึ้น เพื่อนำไปปรับปรุงแผนการป้องกันในอนาคต

ประโยชน์และการนำไปประยุกต์ใช้ในงาน

๑. ด้านการเงินและบัญชี: เพิ่มความระมัดระวังในการเข้าถึงระบบบัญชี การตรวจสอบความถูกต้องของข้อมูล (Integrity) และการป้องกันความลับของข้อมูลทางการเงิน (Confidentiality)

๒. ความตระหนักรู้: สามารถระบุความผิดปกติเบื้องต้นและแจ้งเหตุให้ฝ่ายที่เกี่ยวข้องทราบได้อย่างรวดเร็ว

๓. การทำงานร่วมกัน: เข้าใจบทบาทของตนเองในฐานะส่วนหนึ่งของระบบการบริหารความเสี่ยงองค์กร