สรุปบทเรียนเพื่อการพัฒนาความรู้

เรื่อง การพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น (Basic Cybersecurity Series)

คำอธิบายบทเรียน

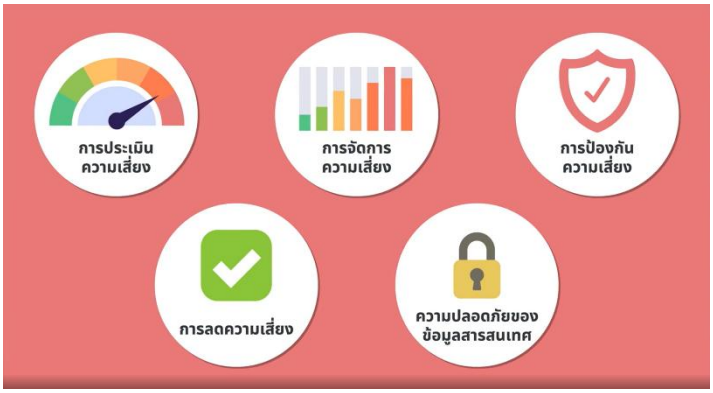
หลักสูตรการพัฒนาทักษะด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) สนับสนุนการเปลี่ยนผ่านสู่รัฐบาลดิจิทัล (สอดคล้องหน่วยความสามารถ CS100 CS200 CS300 CS400 CS500) มุ่งเน้นการดูแลและป้องกันระบบ/บริการ/ผลิตภัณฑ์ ให้คงไว้ซึ่ง ความลับ ความถูกต้องครบถ้วน ความพร้อมใช้งานเพื่อป้องกัน รับมือและลดความเสียหายจากภัยคุกคามทางไซเบอร์เนื้อหาประกอบด้วย 6 หัวข้อ ได้แก่ การประเมินความเสี่ยง (Risk Assessment) การเตรียมพร้อมและความยืดหยุ่นทางไซเบอร์ (Cyber Resilience) กรอบมาตรฐานความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) การป้องกันและประเมินช่องโหว่ (Protect & Vulnerability Assessment) การตรวจสอบและเฝ้าระวัง (Detect) และการตอบสนองและการฟื้นฟู (Respond & Recover)

วัตถุประสงค์

1. ตระหนักและทราบถึงวิธีการป้องกัน Cybersecurity
2. ให้ผู้เรียนเข้าใจความหมายและเห็นถึงความสำคัญของการประยุกต์ใช้งาน Cybersecurity

1. แนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ความมั่นคงปลอดภัยทางไซเบอร์ หมายถึง การปกป้องระบบเครือข่าย อุปกรณ์ และข้อมูลจากการเข้าถึง การใช้งาน การเปิดเผย หรือการทำลายโดยไม่ได้รับอนุญาต หลักพื้นฐานของความมั่นคงปลอดภัยไซเบอร์ คือ แนวคิด CIA Triad ซึ่งประกอบด้วย 3 องค์ประกอบสำคัญ ดังนี้



1) **Confidentiality** คือ การทำให้ข้อมูลเข้าถึงได้เฉพาะผู้ที่ได้รับสิทธิเท่านั้น เช่น การกำหนดสิทธิ์ผู้ใช้งาน การใช้รหัสผ่านที่รัดกุม และการเข้ารหัสข้อมูล หากหลักการนี้ถูกละเมิดจะเกิดเหตุการณ์ข้อมูลรั่วไหล

2) **Integrity** คือ การรักษาความถูกต้องของข้อมูล ไม่ให้ถูกแก้ไขหรือปลอมแปลงโดยไม่ได้รับอนุญาต เช่น การใช้ระบบบันทึกเหตุการณ์ (Log) หรือการใช้ Digital Signature หาก Integrity ถูกทำลาย ความน่าเชื่อถือของข้อมูลจะลดลงทันที

3) **Availability** คือ ความสามารถของระบบในการให้บริการได้อย่างต่อเนื่อง เช่น การมีระบบสำรองข้อมูลหรือศูนย์ข้อมูลสำรอง (Disaster Recovery Site) หากระบบล่มจากการโจมตีแบบ DDoS หรือ Ransomware จะกระทบต่อการดำเนินธุรกิจโดยตรง

นอกจากนี้ “ความเสี่ยง (Risk)” มีบทบาทสำคัญใน Cybersecurity ความเสี่ยงหมายถึงโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหาย ซึ่งเกิดจากการผสมกันของภัยคุกคาม (Threat) ช่องโหว่ (Vulnerability) และผลกระทบ (Impact) ดังนั้น การบริหารความเสี่ยงจึงเป็นกระบวนการสำคัญขององค์กร โดยไม่ใช่หน้าที่ของฝ่าย IT เพียงอย่างเดียว แต่รวมถึงผู้บริหาร ผู้จัดการ พนักงานปฏิบัติการ และผู้ตรวจสอบภายใน

2. การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment)

การประเมินความเสี่ยง เป็นกระบวนการวิเคราะห์และประเมินว่าภัยคุกคามใดอาจเกิดขึ้น และจะส่งผลกระทบต่อองค์กรในระดับใด ขั้นตอนเริ่มต้นจากการระบุทรัพย์สินที่สำคัญขององค์กร เช่น ฐานข้อมูลลูกค้า ระบบบัญชี หรือระบบโครงสร้างพื้นฐาน จากนั้นจึงระบุภัยคุกคามที่อาจเกิดขึ้น เช่น การโจมตีจากแฮกเกอร์ มัลแวร์ หรือความผิดพลาดของมนุษย์ เมื่อทราบภัยคุกคามแล้ว จะต้องมีการวิเคราะห์ช่องโหว่ที่อาจถูกใช้โจมตี และประเมินระดับผลกระทบเพื่อจัดลำดับความสำคัญของความเสี่ยง กระบวนการนี้จะช่วยให้องค์กรสามารถจัดสรรทรัพยากรในการป้องกันได้อย่างมีประสิทธิภาพ

มาตรฐานที่ใช้ในการบริหารความเสี่ยงด้านไซเบอร์ ได้แก่ ISO/IEC 27001 และกรอบการทำงานของ NIST ซึ่งเน้นการจัดการความเสี่ยงเชิงระบบ การใช้มาตรฐานช่วยให้องค์กรมีแนวทางที่ชัดเจนและสามารถประเมินความพร้อมของตนเองได้อย่างเป็นรูปธรรม

3. กรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework)

กรอบมาตรฐานที่ได้รับความนิยมคือ NIST Cybersecurity Framework ซึ่งแบ่งการดำเนินงานออกเป็น 5 ฟังก์ชันหลัก ได้แก่

1) **Identify** คือ การทำความเข้าใจทรัพย์สิน ความเสี่ยง และบริบทขององค์กร หากองค์กรไม่ทราบว่าตนเองมีทรัพย์สินอะไร ก็ไม่สามารถปกป้องได้อย่างเหมาะสม

2) **Protect** คือ การใช้มาตรการป้องกัน เช่น การติดตั้ง Firewall การอัปเดต Patch และการฝึกอบรมพนักงาน

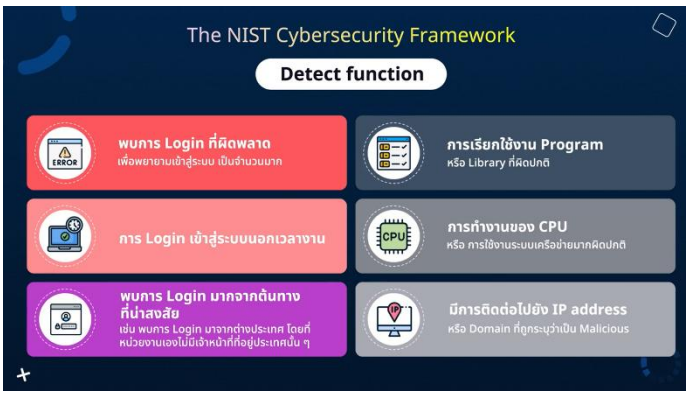
3) **Detect** คือการเฝ้าระวังและตรวจจับเหตุการณ์ผิดปกติ เช่น การเข้าสู่ระบบผิดปกติ หรือการเข้าถึงระบบโดยไม่ได้รับอนุญาต

4) **Respond** คือการดำเนินการเมื่อเกิดเหตุการณ์ เช่น การแยกระบบที่ติดมัลแวร์ การแจ้งทีมงาน และการวิเคราะห์สาเหตุ
5) **Recover** คือการฟื้นฟูระบบให้กลับมาให้บริการได้อย่างต่อเนื่อง เป้าหมายหลักของขั้นตอนนี้ คือการลดระยะเวลาหยุดชะงักของธุรกิจ

4. การป้องกันความเสี่ยงและการประเมินช่องโหว่ (Vulnerability Assessment)

Vulnerability Assessment คือ กระบวนการค้นหาและวิเคราะห์ช่องโหว่ในระบบก่อนที่ผู้ไม่หวังดีจะนำไปใช้โจมตี ขั้นตอนเริ่มจากการสแกนหาช่องโหว่ (Vulnerability Identification) จากนั้นจึงวิเคราะห์ความรุนแรงและสาเหตุของช่องโหว่ (Vulnerability Analysis) ซึ่งเป็นขั้นตอนสำคัญที่ช่วยให้องค์กรเข้าใจระดับความเสี่ยงที่แท้จริง เมื่อวิเคราะห์แล้ว จะต้องจัดทำรายงาน (Reporting) เพื่อเสนอผู้บริหาร และดำเนินการแก้ไข (Remediation) เช่น การอัปเดตซอฟต์แวร์หรือปรับปรุงการตั้งค่าระบบ

5. การตรวจสอบและเฝ้าระวังภัยคุกคาม (Detect)



การตรวจจับภัยคุกคามต้องอาศัยระบบเฝ้าระวังอย่างต่อเนื่อง โดยทีมที่รับผิดชอบมักเรียกว่า Cyber Security Operations Center (CSOC) ซึ่งทำหน้าที่ติดตาม วิเคราะห์และแจ้งเตือนเหตุการณ์ผิดปกติ เช่น การเข้าถึงระบบผ่าน Remote Desktop โดยไม่ได้รับอนุญาต หรือพฤติกรรมที่บ่งชี้การโจมตีแบบ Ransomware การตรวจจับที่รวดเร็วช่วยลดความเสียหายและเพิ่มประสิทธิภาพในการตอบสนอง

6. การเผชิญเหตุภัยคุกคามภัยคุกคามทางไซเบอร์ (Respond) และการฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover)

เมื่อเกิดเหตุการณ์โจมตี องค์กรต้องมีแผนรับมือที่ชัดเจน ขั้นตอนสำคัญ ได้แก่ การแจ้งทีมที่เกี่ยวข้อง การจำกัดความเสียหาย การเก็บหลักฐาน และการวิเคราะห์สาเหตุ สิ่งที่ไม่ควรทำคือการเผยแพร่ข้อมูลเหตุการณ์ผ่านสื่อสังคมออนไลน์โดยไม่ได้รับอนุญาต เพราะอาจสร้างความตื่นตระหนกและกระทบต่อภาพลักษณ์องค์กร หลังควบคุมสถานการณ์ได้แล้ว ต้องเข้าสู่ขั้นตอนการกู้คืนระบบ เป้าหมายคือทำให้ระบบสามารถกลับมาให้บริการได้อย่างต่อเนื่อง การสำรองข้อมูลจึงเป็นกลไกสำคัญ โดยควรใช้แนวทาง 3-2-1 Backup และหลีกเลี่ยงการสำรองข้อมูลไว้ในเครื่องเดียวกับข้อมูลจริง แม้จะแยก Partition ก็ตาม

บทสรุป

หลักสูตร Basic Cybersecurity Series เป็นแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยการกำหนดนโยบาย การควบคุมการเข้าถึง และการสร้างความตระหนักรู้ของบุคลากร รวมถึงการประเมินความเสี่ยงเพื่อระบุภัยคุกคาม ช่องโหว่ และผลกระทบ จากนั้นใช้กรอบมาตรฐาน Cybersecurity Framework ที่ประกอบด้วย Identify, Protect, Detect, Respond และ Recover เป็นแนวทางดำเนินงานอย่างเป็นระบบ ในตอนขั้น Protect จะมีการประเมินช่องโหว่ เพื่อค้นหา วิเคราะห์ รายงาน และแก้ไขจุดอ่อน ขั้น Detect จะมีการเฝ้าระวังและตรวจจับเหตุผิดปกติอย่างรวดเร็ว ส่วน Respond และ Recover มุ่งควบคุมเหตุการณ์ ฟื้นฟูระบบ และทำให้บริการกลับมาใช้งานได้อย่างต่อเนื่อง หลักสูตรนี้จึงเน้นการบริหารความเสี่ยงแบบครบวงจร เพื่อสร้างความมั่นคงปลอดภัยอย่างยั่งยืน

สรุปบทเรียนเพื่อการพัฒนาความรู้ โดย นางสาวกันยารัตน์ทะเทพ
นักวิเคราะห์นโยบายและแผนปฏิบัติการ
กลุ่มพัฒนาระบบบริหาร

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

กันยารัตน์ ทะเทพ

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Basic Cybersecurity Series :

หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

จำนวนชั่วโมงการเรียนรู้ 1:30 **ชั่วโมง**

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 24 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

e370c809