Basic Cybersecurity Series : หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

โดย นางสาวธัญญลักษณ์ ชัยวรพล
นักวิชาการแผนที่ภาพถ่ายปฏิบัติการ

วัตถุประสงค์

๑. เพื่อพัฒนาทักษะทางด้าน Cybersecurity เพิ่มมากขึ้น

๒. ให้ผู้เรียนเข้าใจความหมายและให้ผู้เรียนเห็นถึงความสำคัญของการประยุกต์ใช้งาน Cybersecurity

สรุปเนื้อหา การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment)

ความเสี่ยง คือ เหตุการณ์ การกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบ หรือ สร้างความเสียหายความล้มเหลวหรือลดโอกาสที่จะบรรลุเป้าหมายและวัตถุประสงค์ ทั้งในระดับองค์กร ระดับหน่วยงาน และระดับบุคคลได้

การบริหารความเสี่ยง (Risk Management) หมายถึง กลวิธีที่เป็นเหตุเป็นผลที่นำมาใช้ในการวิเคราะห์ ประเมิน จัดการ ติดตาม และสื่อสารสิ่งที่เกี่ยวข้องกับกิจกรรม หน่วยงาน/ฝ่ายงาน หรือกระบวนการดำเนินงานขององค์กร เพื่อช่วยลดความสูญเสียในการไม่บรรลุเป้าหมายให้เหลือน้อยที่สุด และเพิ่มโอกาสแก่องค์กรมากที่สุด

Basic Cybersecurity

๑. การปกป้องข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลเช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ และข้อมูลการเงินเป็นเป้าหมายหลักของการโจมตีทางไซเบอร์ การถูกขโมยข้อมูลส่วนบุคคลสามารถนำไปสู่การสูญเสียทางการเงินหรือการถูกนำไปใช้ในทางที่ผิด

๒. การป้องกันการโจมตีทางไซเบอร์ การป้องกันการโจมตีทางไซเบอร์ แนวคิดหลักจะเป็นการดำเนินการเพื่อให้คงไว้ซึ่งหลัก CIA คือ Confidentiality Integrity และ Availability ของข้อมูลและระบบที่ให้บริการเป็นหลัก

๓. การรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ การป้องกันคุกคามทางไซเบอร์นั้น ไม่ว่าเราจะลงทุนป้องกันและดำเนินการป้องกันดีแค่ไหน ก็ไม่สามารถรับรองได้ว่าสินทรัพย์ของเราจะปลอดภัย ๑๐๐%

๔. การสร้างความเชื่อมั่นและความน่าเชื่อถือ ในโลกธุรกิจ ความปลอดภัยทางไซเบอร์มีความสำคัญต่อการสร้างความเชื่อมั่นให้กับลูกค้าและพันธมิตรทางธุรกิจ องค์กร ที่มีมาตรการรักษาความปลอดภัยที่ดีจะได้รับความเชื่อถือจากลูกค้า

สภาพแวดล้อมความเสี่ยงภัยคุกคามทางไซเบอร์ แบ่งออกเป็น ๒ ทาง

๑. สภาพแวดล้อมภายนอก ได้แก่

- Socio-cultural Factors ความสลับซับซ้อนทางสังคม โครงสร้างประชากร การศึกษา อาชีพ อื่น ๆ
- Economic Factors ภาวะทางเศรษฐกิจ การจ้างงาน อัตราดอกเบี้ย ฯลฯ
- Political and Legal Factors เสถียรภาพของรัฐบาล นโยบายรัฐ กฎหมาย ฯลฯ
- Technological Factors นวัตกรรม ความมีอยู่ของเทคโนโลยี ฯลฯ

๒. สภาพแวดล้อมภายใน ได้แก่

- Structure and Policy โครงสร้างองค์กร กลยุทธ์ ฯลฯ
- Service ผลผลิตและผลลัพธ์ ความพึงพอใจของผู้รับบริการ ฯลฯ
- Manpower อัตรากำลัง คุณภาพบุคลากร การบริหารบุคคล ฯลฯ
- Money ประสิทธิภาพด้านการเงิน การระดมทุน
- Materials วัสดุ อุปกรณ์ เครื่องจักร ฯลฯ
- Management กระบวนการ ภาวะความเป็นผู้นำ วัฒนธรรมองค์กร สารสนเทศ ฯลฯ

ความสำคัญของจัดการบริหารความเสี่ยง

๑. เพื่อส่งเสริมให้องค์กรมีการบูรณาการระหว่างการบริหารความเสี่ยงกับควบคุมภายใน

๒. เพื่อสะท้อนการพัฒนาในด้านการกำกับดูแลที่ดีขององค์กร การกำหนดวัตถุประสงค์และยุทธศาสตร์องค์กรที่ชัดเจน

๓. เพื่อให้ฝ่ายบริหารเกิดความมั่นใจ ว่าการดำเนินงานจะบรรลุวัตถุประสงค์ได้ตามเป้าหมาย

๔. เพื่อเป็นกลไก ในการผลักดันให้องค์กรมีแนวทางการบริหารความเสี่ยง

การป้องกันความเสี่ยง (Protect) โดยการประเมินช่องโหว่ (Vulnerability Assessment)

การประเมินช่องโหว่ (Vulnerability Assessment) คือกระบวนการที่ใช้ในการตรวจสอบและระบุช่องโหว่ที่มีอยู่ในระบบหรือแอปพลิเคชัน โดยใช้เครื่องมือตรวจสอบช่องโหว่และเทคนิคการสแกนเพื่อค้นหาปัญหาด้านความปลอดภัยซึ่งกระบวนการนี้ช่วยให้ทราบถึงช่องโหว่ที่เปิดเผยในระบบหรือแอปพลิเคชันจนนำไปสู่วิธีการแก้ไขได้อย่างถูกจุดเพื่อเพิ่มความปลอดภัย

Vulnerability Scanning Tool คือ ซอฟต์แวร์อัตโนมัติที่ใช้ตรวจสอบ (Scan) ระบบเครือข่าย แอปพลิเคชัน และโครงสร้างพื้นฐานไอที เพื่อค้นหาช่องโหว่ (Vulnerability) เพื่อตรวจสอบความปลอดภัยระบบเครือข่ายค้นหาช่องโหว่ที่ใช้งานภายในองค์กร เช่น ระบบปฏิบัติการ (OS) ซอฟต์แวร์ อุปกรณ์ Network อุปกรณ์ Security ฯลฯ ซึ่งมันเป็นเรื่องสำคัญที่ใช้ระบุระดับความรุนแรงของช่องโหว่ ที่เกิดขึ้นตามการอ้างอิงของ CVE และ CVSS

ประโยชน์ของ Vulnerability Assessment คือ

๑. ช่วยในการประเมินระดับความเสี่ยงที่มาจากช่องโหว่

๒. ช่วยในการสร้างรายงานที่รวมข้อมูลเกี่ยวกับช่องโหว่ที่พบ

๓. ช่วยในการตรวจสอบว่าระบบสอดคล้องกับมาตรฐาน

๔. ช่วยในการค้นพบและแก้ไขช่องโหว่และปัญหาความปลอดภัย

ขั้นตอนการรับมือภัยคุกคามทางไซเบอร์

๑. การเตรียมการ เช่น การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ การตั้งทีมตอบสนองต่อเหตุการณ์ การฝึกอบรมพนักงานด้านการรับรู้ความปลอดภัยทางไซเบอร์ การเตรียมเครื่องมือต่าง ๆ

๒. การระบุภัยคุกตาม ขั้นตอนนี้เกี่ยวข้องกับการตรวจจับเหตุการณ์ด้านความปลอดภัยที่อาจจะเกิดขึ้น ซึ่งสามารถเกิดขึ้นได้ ผ่านการแจ้งเตือนจากระบบที่ติดตั้งไว้

๓. การควบคุม เป้าหมายในขั้นตอนนี้คือการหยุดการโจมตีและลดความเสียหายให้น้อยที่สุด เช่น การตัดการเชื่อมต่อกับระบบเครือข่าย

๔. การกำจัดภัยคุกคามที่ตรวจสอบ เช่น การลบไฟล์ Malware เป็นต้น

การนำองค์ความรู้ไปปรับใช้ในการปฏิบัติงาน

สามารถเริ่มต้นจากการจัดการรหัสผ่านอุปกรณ์คอมพิวเตอร์ และโปรแกรมต่าง ๆ อย่างเหมาะสม นอกจากนี้ การใช้งานอีเมลและอินเทอร์เน็ตอย่างระมัดระวังถือเป็นอีกหนึ่งแนวทางสำคัญ ซึ่งควรตรวจสอบแหล่งที่มาของอีเมล ลิงก์ และไฟล์แนบก่อนเปิดใช้งาน หลีกเลี่ยงการคลิกลิงก์จากแหล่งที่ไม่น่าเชื่อถือ จะช่วยลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

ประโยชน์ที่ได้รับ

ประโยชน์ต่อตนเอง

การมีความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ช่วยให้สามารถใช้งานเทคโนโลยีดิจิทัลได้อย่างปลอดภัยและมีสติ รู้จักป้องกันข้อมูลส่วนบุคคล เช่น รหัสผ่าน ข้อมูลทางการเงิน และข้อมูลส่วนตัวจากการถูกโจรกรรมหรือหลอกลวงทางออนไลน์ นอกจากนี้ยังช่วยให้สามารถตรวจสอบและหลีกเลี่ยงภัยคุกคามทางไซเบอร์ เช่น อีเมลหลอกลวง มัลแวร์ และเว็บไซต์ปลอม ลดความเสี่ยงจากความเสียหายที่อาจเกิดขึ้นทั้งด้านทรัพย์สินและชื่อเสียง

ประโยชน์ต่อองค์กร

ในระดับองค์กร ความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ช่วยลดความเสี่ยงจากการรั่วไหลของข้อมูลและการโจมตีทางไซเบอร์ พนักงานที่มีความรู้และความตระหนักด้านความปลอดภัยจะสามารถปฏิบัติงานได้อย่างถูกต้องตามนโยบายขององค์กร ช่วยป้องกันความเสียหายต่อระบบงาน ทรัพย์สิน และภาพลักษณ์ขององค์กร อีกทั้งยังช่วยเสริมสร้างความเชื่อมั่นให้กับผู้ใช้บริการและผู้มีส่วนได้ส่วนเสีย

ประโยชน์ต่อสาธารณะ

ช่วยให้ข้อมูลส่วนบุคคล ของผู้มาติดต่อราชการไม่เกิดการรั่วไหล และช่วยลดปัญหาอาชญากรรมทางไซเบอร์

แหล่งที่มา

หลักสูตร : Basic Cybersecurity Series : หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

บรรยายโดย : นางสาวศรีสุดา แซ่เฮ้ง และ นายธงไชย จารุสุรเกษม

สถาบัน/หน่วยงาน/ระบบ : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

รูปแบบหลักสูตร : การเรียนรู้ออนไลน์ TDGA e-Learning

ช่วงเวลาการฝึกอบรม : กุมภาพันธ์ ๒๕๖๙