สรุปการฝึกอบรม หลักสูตร พัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

(Basic Cybersecurity Series)

ผ่านระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ LDD e-Training

ผู้รับการฝึกอบรม : นางสาวจรดจันทร์ ชำนาญกิจ
ตำแหน่ง : นักวิชาการเผยแพร่ปฏิบัติการ
สังกัด : กลุ่มงานพิพิธภัณฑ์ดิน สำนักงานเลขานุการกรม

วัตถุประสงค์การเรียนรู้

๑. เพื่อให้ผู้เข้ารับการอบรม มีความรู้และความเข้าใจเกี่ยวกับการพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์มากขึ้น

๒. เพื่อให้สามารถปฏิบัติงานได้ตามวัตถุประสงค์ของหน่วยงาน

โดยมีหัวข้อบทเรียนตามหลักสูตร ดังนี้

<u>ความสำคัญของความมั่นคงปลอดภัยทางไซเบอร์</u>

ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) คือการป้องกันและควบคุมระบบสารสนเทศ อุปกรณ์คอมพิวเตอร์และเครือข่าย จากภัยคุกคามต่าง ๆ ที่อาจก่อให้เกิดความเสียหายต่อข้อมูลและการให้บริการขององค์กร ภัยคุกคามทางไซเบอร์อาจเกิดจากผู้ไม่หวังดี เช่น แฮกเกอร์ มัลแวร์ หรือการโจมตีทางเครือข่าย

การรักษาความมั่นคงปลอดภัยไซเบอร์ หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศ กระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ “ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวของ และเป็นภัยอันตราย ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

<u>ประเภทของภัยคุกคามทางไซเบอร์</u>

ภัยคุกคามทางไซเบอร์มีหลายรูปแบบ คือ

๑. เนื้อหาที่เป็นภัยคุกคาม (Abusive Content) ภัยคุกคามที่เกิดจากการใช้ข้อมูลที่ไม่เป็นความจริงหรือไม่เหมาะสม (Abusive Content) เพื่อทำลายความน่าเชื่อถือของบุคคลหรือสถาบัน เพื่อก่อให้เกิดความไม่สงบ

หรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย เช่น ลามก อนาจาร หมิ่นประมาท และรวมถึงการ โฆษณาขายสินค้าต่างๆ ทางอีเมลที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้นๆ (SPAM)

๒. การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability) ภัยคุกคามที่เกิดจากการโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อทำให้บริการต่างๆของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบ ตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้ ภัยคุกคามอาจจะเกิดจากการโจมตีที่บริการของระบบโดยตรง เช่น การโจมตีประเภท DOS (Denial of Service) แบบต่าง ๆ หรือการโจมตีโครงสร้างพื้นฐานที่สนับสนุนการให้บริการของ ระบบ เช่น อาคาร สถานที่ ระบบไฟฟ้า ระบบปรับอากาศ

๓. การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) ภัยคุกคามที่เกิดจากการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งาน ระบบ หรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตโดยมีวัตถุประสงค์เพื่อแสวงหาผลประโยชน์ของตนเองหรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์

๔. ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering) ภัยคุกคามที่เกิดจากความพยายามในการรวบรวมข้อมูลจุดอ่อนของระบบของผู้ไม่ประสงค์ดี ด้วยการเรียกใช้บริการต่างๆที่ อาจจะเปิดไว้บนระบบ รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่าย (Sniffing) และการล่อลวงหรือใช้เล่ห์กลต่างๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ (Social Engineering)

๕. การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security) ภัยคุกคามที่เกิดจากการที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญ (Unauthorized Access) หรือเปลี่ยนแปลงแก้ไขข้อมูล (Unauthorized modification) ได้

๖. ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts) ภัยคุกคามที่เกิดจากความพยายามบุกรุก /เจาะเข้าระบบ (Intrusion Attempts) ทั้งที่ผ่านจุดอ่อนหรือช่องโหว่ที่เป็นที่รู้จักในสาธารณะ (CVE Common Vulnerabilities and Exposures) หรือผ่านจุดอ่อนหรือช่อง โหว่ใหม่ที่ยังไม่เคยพบมาก่อนเพื่อจะได้เข้าครอบครองหรือทำให้เกิดความขัดข้องกับบริการต่าง ๆ ของระบบภัยคุกคามนี้ รวมถึงความพยายามจะบุกรุก/เจาะระบบ ผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่าน (Login) ด้วยวิธีการสุ่มข้อมูล

๗. การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions) ภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้สำเร็จ (Intrusions) และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต

๘. โปรแกรมไม่พึงประสงค์ (Malicious Code) ภัยคุกคามที่เกิดจากโปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้นเพื่อส่งผลลัพธ์ที่ไม่พึงประสงค์กับผู้ใช้งานหรือระบบ (Malicious Code) เพื่อทำให้เกิดความขัดข้องหรือเสียหายกับระบบที่โปรแกรมหรือซอฟต์แวร์ประสงค์ร้ายนี้ติดตั้งอยู่ โดยปกติโปรแกรมหรือ ซอฟต์แวร์ประสงค์ร้ายประเภทนี้ต้องอาศัยผู้ใช้งานเป็นผู้เปิดโปรแกรมหรือ ซอฟต์แวร์ก่อน จึงจะสามารถติดตั้งตัวเองหรือ ทำงานได้ เช่น Virus

๙. ภัยคุกคามอื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น (Other) ภัยคุกคามประเภทอื่น ๆ นอกเหนือจากที่กำหนดไว้ข้างต้น ระบุไว้เพื่อเป็นตัวชี้วัดถึงภัยคุกคามประเภทใหม่หรือไม่สามารถจัดประเภท ได้ตามที่ระบุไว้ข้างต้น โดยถ้าจำนวนภัยคุกคามอื่น ๆ ในข้อนี้มีจำนวนมากขึ้น แสดงถึงความจำเป็นที่จะต้องปรับปรุงการจัดแบ่งประเภทภัยคุกคามนี้ใหม่

<u>การแบ่งประเภทภัยคุกคามทางไซเบอร์</u>

๑. Application/Service/ OS configuration problem เหตุการณ์ที่เกิดจากการ Configuration แอปพลิเคชัน/การให้บริการ/ระบบปฏิบัติการ ที่ผิดพลาด

๒. Denial of Service (DoS) เหตุการณ์ที่ผู้บุกรุกส่งข้อมูล และ packet จำนวนมากไปยังเครือข่าย หรือเครื่องของหน่วยงาน เพื่อให้เครื่องให้บริการหยุดชะงัก

๓. Fraud เหตุการณ์ที่เกิดจากการฉ้อฉลฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบ หรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์

๔. Information Gathering เหตุการณ์ที่ตรวจพบความพยายามของผู้บุกรุกในการค้นหาข้อมูลสำคัญเพื่อใช้สำหรับการโจมตีเข้าสู่ระบบ

๕. Information Leak เหตุการณ์ที่ตรวจพบการรั่วไหลของข้อมูลสำคัญจากช่องทางต่างๆ เช่น Social Media ที่อาจจะส่งผลกระทบต่อความมั่นคงปลอดภัย

๖. Malware Detected การบุกรุกที่เกิดจากการโจมตีของมัลแวร์ไปยังเครือข่าย และเครื่องให้บริการของหน่วยงาน ได้แก่ Backdoor, Trojan, Virus, Worm และ Botnet

๗. Server Compromise เหตุการณ์ที่ตรวจพบว่าเครื่องให้บริการ (Server) ของหน่วยงานถูกบุกรุกและเข้าถึงโดยไม่ได้รับอนุญาต โดยผู้บุกรกเป็นที่เรียบร้อย

๘. Service Unavailable การทำให้บริการมีปัญหาหรือเกิดเหตุขัดข้อง

๙. Suspicious Activity การเชื่อมต่อข้อมูล และ Traffic ที่ผิดปกติ และมีความเชื่อมโยงที่จะเป็นการบุกรุกระบบ

๑๐. Web Compromise Web Application หรือเว็บไซต์ จะถูกยึดครองโดยไม่ได้รับอนุญาต

<u>แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับบุคคลและหน่วยงาน</u>

สำหรับบุคคล

๑. ระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าไปยังเว็บไซต์ที่ไม่เหมาะสม ไม่เปิดไฟล์ที่ไม่มีการตรวจสอบแน่ชัดหรือเปิดไฟล์จากบุคคลที่ไม่รู้จัก และระมัดระวังการเปิดไฟล์ผ่าน Social Media ทั้งนี้เพื่อหลีกเลี่ยงพวกมัลแวร์

๒. ไม่ใช้รหัสผ่านบน โลก cyber เป็นรหัสชุดเดียวกันทุกระบบและไม่บันทึกรหัสผ่านไว้แบบอัตโนมัติ

๓. ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัยและพิจารณาข้อมูลก่อนเผยแพร่เพื่อป้องกันตนเองเป็นต้นตอในการส่งแพร่กระจายไวรัส

สำหรับหน่วยงาน

๑. ตรวจสอบและยืนยันสิทธิการเข้าระบบที่สำคัญของบัญชีผู้ใช้ให้สอดคล้องกับความจำเป็นในการเข้าถึงระบบและข้อมูล

๒. เพิ่มมาตรการป้องกันเว็บไซต์สำคัญด้วยระบบป้องกันการโจมตีของ ไวรัส Web Application Firewall หรือ DDos Protection แจ้งเจ้าหน้าที่ของหน่วยงานให้เพิ่มความระมัดระวังในการใช้งานอินเตอร์เน็ตโดยหลีกเลี่ยงความไม่เหมาะสม และป้องกันข้อความจาก Social Media

๓. หากพบสิ่งน่าสงสัยว่าระบบถูกโจมตี เช่น ไม่สามารถเข้าใช้งานระบบ/เว็บไซต์ได้ หรือมีความล่าช้ากว่าปกติ ควรตรวจสอบการ login ย้อนหลังทุกๆ เดือน

๔. ตั้งค่าระบบงานที่สำคัญให้บันทึกเหตุการณ์ต่าง ๆ ตามที่กฎหมายกำหนดไว้

ดังนั้นในการแก้ไขหรือป้องกันทางการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับ บุคคลและหน่วยงาน ผู้บริหารต้องมีส่วนร่วมในการรับทราบและให้แนวทางในการแก้ปัญหาให้ถูกต้องเพื่อให้สร้างความมั่นคงทางไซเบอร์ และให้ผู้ใช้มีความรู้และความเข้าใจในปัญหาจากการคุกคามว่าเกิดขึ้นได้อย่างไร ต้นตอเกิดจากอะไร เพราะหากเกิดช่องโหว่ในระบบ ก็สามารถถูกแฮกเกอร์เจาะเข้าระบบได้เช่นกัน ผู้ใช้งานทุกคนควรมีความระมัดระวังในการใช้งานระบบไซเบอร์ ตระหนักรู้ในเรื่องของความมั่นคง ปลอดภัย และควรมีไหวพริบในขณะที่กำลังเจอกับปัญหา ถือเป็นการรู้จักป้องกันการก่อให้เกิดปัญหาทางความมั่นคงทางไซเบอร์อีกด้วย เพื่อป้องกันการเกิดเหตุการณ์ที่ไม่คาดคิดที่จะเกิดขึ้นได้ตลอดเวลา

การพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นสิ่งจำเป็นสำหรับบุคลากรทุกระดับความเข้าใจในภัยคุกคาม การประเมินความเสี่ยง การปฏิบัติเมื่อเกิดเหตุ และการจัดทำแผนรับมือ เป็นองค์ประกอบสำคัญที่ช่วยให้องค์กรสามารถป้องกันและตอบสนองต่อภัยไซเบอร์ได้อย่างมีประสิทธิภาพ

หลักสูตรนี้ช่วยให้บุคลากรมีความรู้พื้นฐาน สามารถประเมินความเสี่ยง ป้องกัน ตรวจจับ และตอบสนองต่อเหตุการณ์ได้อย่างเหมาะสม สอดคล้องกับมาตรฐานสากลและแนวทางปฏิบัติขององค์กร
