หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

Basic Cybersecurity Series

ปัจจุบันเทคโนโลยีสารสนเทศและอินเทอร์เน็ตได้เข้ามามีบทบาทในชีวิตประจำวันของผู้คนและองค์กรอย่างลึกซึ้ง ตั้งแต่การทำงาน การศึกษา การสื่อสาร การซื้อขายสินค้า ไปจนถึงการทำธุรกรรมทางการเงิน อย่างไรก็ตาม ความก้าวหน้าทางเทคโนโลยีดังกล่าวก็มาพร้อมกับความเสี่ยงด้านภัยคุกคามไซเบอร์ (Cyber Threats) ที่มีความซับซ้อนมากขึ้นเรื่อย ๆ การพัฒนาทักษะด้านความมั่นคงปลอดภัยไซเบอร์จึงไม่ใช่เรื่องของผู้เชี่ยวชาญเพียงอย่างเดียว แต่เป็นสิ่งที่ผู้ใช้ทุกคนจำเป็นต้องเรียนรู้ เพื่อสร้างความปลอดภัยทั้งในระดับบุคคล องค์กร และสังคมโดยรวม

หลักสูตร Basic Cybersecurity Series ถูกออกแบบมาเพื่อมุ่งเน้นการสร้างความเข้าใจเบื้องต้นเกี่ยวกับแนวคิด ภัยคุกคาม และวิธีปฏิบัติที่ถูกต้อง เพื่อป้องกันความเสี่ยงและรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นได้ตลอดเวลา

ความหมายและความสำคัญของความมั่นคงปลอดภัยไซเบอร์

ประเภทของภัยคุกคามทางไซเบอร์

๑. เนื้อหาที่เป็นภัยคุกคาม (Abusive Content) ภัยคุกคามที่เกิดจากการใช้/เผยแพร่ข้อมูลที่ไม่ เป็นจริงหรือไม่เหมาะสม (Abusive Content) เพื่อท าลายความน่าเชื่อถือของบุคคลหรือสถาบัน เพื่อ ก่อให้เกิดความไม่สงบ หรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย เช่น ลามก อนาจาร หมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่างๆ ทางอีเมลที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้นๆ (SPAM)

๒. การโจมตีสภาพความพร้อมใช้งานของ ระบบ (Availability) ภัยคุกคามที่เกิดจากการโจมตี สภาพความพร้อมใช้งานของระบบ เพื่อท าให้บริการต่างๆของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบ ตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่ สามารถให้บริการต่อไปได้ ภัยคุกคามอาจจะเกิดจากการโจมตีที่บริการ ของระบบโดยตรง เช่น การโจมตีประเภท DOS (Denial of Service) แบบต่างๆ หรือการโจมตีโครงสร้างพื้นฐานที่สนับสนุนการให้บริการของ ระบบ เช่น อาคารสถานที่ ระบบไฟฟ้า ระบบปรับอากาศ

๓. การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อ ผลประโยชน์ (Fraud) ภัยคุกคามที่เกิดจากการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งาน

ระบบ หรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ ของตนเอง หรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์

๔. ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering) ภัยคุกคามที่เกิดจากความพยายามในการรวบรวมข้อมูลจุดอ่อนของ ระบบของผู้ไม่ประสงค์ดี(Scanning) ด้วยการเรียกใช้บริการต่างๆที่ อาจจะเปิดไว้บนระบบ เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการ ระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชี ชื่อผู้ใช้งาน (User Account) ที่ มีอยู่บนระบบเป็นต้น รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจร บน ระบบเครือข่าย (Sniffing) และการล่อลวงหรือใช้เล่ห์กลต่างๆ เพื่อให้ ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญ ของระบบ (Social Engineering)

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

๖. ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts) ภัยคุกคามที่เกิดจากความพยายาม จะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) ทั้งที่ผ่านจุดอ่อนหรือช่องโหว่ที่เป็นที่รู้จักในส าธารณะ (CVECommon Vulnerabilities and Exposures) หรือผ่านจุดอ่อนหรือช่อง โหว่ใหม่ที่ยังไม่เคยพบมาก่อน เพื่อจะได้เข้าครอบครองหรือท าให้เกิด ความขัดข้องกับบริการต่างๆของระบบ ภัยคุกคามนี้รวมถึงความ พยายาม จะบุกรุก/เจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและ รหัสผ่าน (Login) ด้วยวิธีการ สุ่ม/เดาข้อมูล หรือวิธีการทดสอบรหัสผ่าน ทุกค่า (Brute Force)

๗. การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions) ภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้า ระบบได้สำเร็จ (Intrusions) และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต

๘. โปรแกรมไม่พึงประสงค์ (Malicious Code) ภัยคุกคามที่เกิดจากโปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้นเพื่อส่งให้เกิดผลลัพธ์ที่ไม่พึงประสงค์ กับผู้ใช้งานหรือระบบ (Malicious Code) เพื่อท าให้เกิดความ ขัดข้องหรือเสียหายกับระบบที่โปรแกรมหรือ ซอฟต์แวร์ประสงค์ร้ายนี้ติดตั้งอยู่ โดยปกติโปรแกรมหรือ ซอฟต์แวร์ ประสงค์ร้ายประเภทนี้ต้องอาศัยผู้ใช้งานเป็นผู้เปิดโปรแกรมหรือ ซอฟต์แวร์ก่อน จึงจะสามารถ ติดตั้งตัวเองหรือทำงานได้ เช่น Virus, Worm, Trojan หรือ Spyware ต่างๆ

๙. ภัยคุกคามอื่นๆ นอกเหนือจากที่ก าหนดไว้ข้างต้น (Other) ภัยคุกคามประเภทอื่นๆ นอกเหนือจากที่ก าหนดไว้ข้างต้น ระบุไว้เพื่อเป็น ตัวชี้วัดถึงภัยคุกคามประเภทใหม่หรือไม่ส ามารถจัดประเภท ได้ตามที่ระบุ ไว้ข้างต้น โดยถ้าจำนวนภัยคุกคามอื่นๆ ในข้อนี้มีจำนวนมากขึ้น แสดงถึง ความจำเป็นที่จะต้องปรับปรุงการจัดแบ่งประเภทภัยคุกคามนี้ใหม่

การแบ่งประเภทภัยคุกคามทางไซเบอร์

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

๒. Denial of Service (DoS) เหตุการณ์ที่ผู้บุกรุกส่งข้อมูล และ packet จ านวนมากไปยัง เครือข่าย หรือเครื่องของหน่วยงาน เพื่อให้เครื่องให้บริการหยุดชะงัก

๓. Fraud เหตุการณ์ที่เกิดจากการฉ้อฉลฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์(Fraud) สามารถ เกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบ หรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้ าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์

๔. Information Gathering เหตุการณ์ที่ตรวจพบความพยายามของผู้บุกรุกในการค้นหาข้อมูล ส าคัญ เพื่อใช้ส าหรับการโจมตีเข้าสู่ระบบ

๕. Information Leak เหตุการณ์ที่ตรวจพบการรั่วไหลของข้อมูลส าคัญจากช่องทางต่างๆ เช่น Social Media ที่อาจจะส่งผลกระทบต่อความมั่นคงปลอดภัย

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

๗. Server Compromise เหตุการณ์ที่ตรวจพบว่าเครื่องให้บริการ (Server) ของหน่วยงานถูกบุก รุก และเข้าถึงโดยไม่ได้รับอนุญาต โดยผู้บุกรกเป็นที่เรียบร้อย

๘. Service Unavaliable การท าให้บริการมีปัญหาหรือเกิดเหตุขัดข้อง จนไม่สามารถให้บริการได้

๙. Suspicious Activity การเชื่อมต่อข้อมูล และ Traffic ที่ผิดปรกติ และมีความเชื่อมโยงที่จะเป็น การบุกรุกระบบ

๑๐. Web Compromise Web Application หรือเว็บไซต์ ถูกยึดครองโดยไม่ได้รับอนุญาต แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับบุคคลและหน่วยงาน

บทสรุป

หลักสูตร Basic Cybersecurity Series มุ่งเน้นการสร้างพื้นฐานความรู้และทักษะที่จำเป็นด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ผู้เข้าอบรม ทุกคนจะได้เรียนรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่พบบ่อย หลักการป้องกันพื้นฐาน และวิธีการตอบสนองต่อเหตุการณ์ที่เกิดขึ้นจริง

การปฏิบัติตามแนวทางที่ถูกต้อง เช่น การใช้รหัสผ่านที่ปลอดภัย การอัปเดตระบบ การสำรองข้อมูล และการตระหนักรู้ถึงความเสี่ยง จะช่วยลดโอกาสในการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ได้อย่างมาก สิ่งสำคัญที่สุดคือการสร้าง วัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Culture) ให้เป็นส่วนหนึ่งของการใช้ชีวิตประจำวัน เพื่อให้ทั้งบุคคลและองค์กรสามารถดำเนินกิจกรรมทางดิจิทัลได้อย่างปลอดภัย มั่นคง และยั่งยืน

สรุปบทเรียนโดย : นางสาวกานต์สิริ เคนเหลื่อม ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ

สถานีพัฒนาที่ดินสุรินทร์ สำนักงานพัฒนาที่ดินเขต ๓

(นางสาวกานต์สิริ เคนเหลื่อม)

นักวิชาการเกษตรปฏิบัติการ

DGA
DIGITAL GOVERNMENT DEVELOPMENT AGENCY

TDGA
THAILAND DIGITAL GOVERNMENT ACADEMY

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ กานต์สิริ เคนเหลื่อม

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Basic Cybersecurity Series : หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ไว้ ณ วันที่ 27 สิงหาคม 2568

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2025-08-27T10:28:40.402+07:00

c8b7d123