สรุปบทเรียนจากการพัฒนาความรู้

รอบการประเมินที่ 2
ปีงบประมาณ พ.ศ. 2568

Basic Cybersecurity Series : หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

จัดทำโดย นายฉัตรชัย เจริญสรรพสุข
ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ

ในยุคที่เทคโนโลยีและอินเทอร์เน็ต เข้ามามีบทบาทสำคัญในการดำเนินชีวิตประจำวัน ความมั่นคงปลอดภัยทางไซเบอร์เป็นสิ่งที่ไม่สามารถมองข้ามได้ ไม่ว่าจะเป็นในองค์กรขนาดใหญ่หรือบุคคลทั่วไป การรักษาความปลอดภัยของข้อมูล ถือเป็นหัวใจสำคัญที่ช่วยป้องกันความเสี่ยงจากการถูกโจมตีทางไซเบอร์ได้ในหลายรูปแบบ เพื่อปกป้องข้อมูลและทรัพย์สินทางดิจิทัลของบุคคลและองค์กร

การปกป้องข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ และข้อมูลทางการเงิน เป็นเป้าหมายหลักของการโจมตีทางไซเบอร์ การถูกขโมยข้อมูลส่วนบุคคล สามารถนำไปสู่การสูญเสียทางการเงินหรือการถูกนำไปใช้ในทางที่ผิดได้ การมีพื้นฐานของความมั่นคงทางปลอดภัยทางไซเบอร์ที่ดี เช่น การใช้งานรหัสผ่านที่เข้มแข็ง การเปิดใช้งานการยืนยันตัวตนหลายรูปแบบ การรักษาความลับข้อมูลส่วนบุคคล เป็นต้น สิ่งเหล่านี้จะช่วยลดความเสี่ยงในการถูกโจมตีได้ไม่มากก็น้อย

การป้องกันการโจมตีทางไซเบอร์

เน้นยึดถือตามหลักแนวคิดที่จะเป็นการดำเนินการเพื่อให้คงไว้ซึ่ง**หลัก CIA คือ การรักษาความลับของข้อมูล (Confidentiality) การทำให้ข้อมูลพร้อมใช้งาน (Availability) และการแน่ใจว่าข้อมูลมีความถูกต้อง (Integrity)** ของข้อมูลและระบบที่ให้บริการเป็นหลัก

การดำเนินการให้ระบบสารสนเทศมีความมั่นคงปลอดภัย ควรจะดำเนินการตามหลักการประเมินความเสี่ยง เพื่อให้แน่ใจได้ว่า เราจะปกป้องสินทรัพย์ได้อย่างปลอดภัยด้วยการลงทุนที่เหมาะสม และต้องดำเนินการป้องกันให้รอบด้าน ไม่ว่าจะเป็นทางด้านข้อมูล ระบบสารสนเทศ หรือข้อมูลส่วนบุคคล ที่อาจถูกผู้ไม่หวังดีเข้ามาโจมตีได้

การรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์

การป้องกันภัยคุกคามทางไซเบอร์นั้น ไม่ว่าเราจะลงทุนป้องกันโดยทรัพยากรมากแค่ไหน หรือดำเนินการป้องกันได้ดีแค่ไหน **ไม่สามารถรับรองได้ว่าสินทรัพย์ของเราจะปลอดภัย ๑๐๐%** เราจึงต้องยึดแนวทางปฏิบัติที่เป็นมาตรฐานหรือแนวทางการประเมินความเสี่ยง เพื่อให้เกิดความแน่ใจว่าเราได้ป้องกันสินทรัพย์ที่มีได้ดีเพียงพอ

การสร้างความเชื่อมั่นและความน่าเชื่อถือ

ในโลกธุรกิจ ความปลอดภัยทางไซเบอร์มีความสำคัญต่อการสร้างความเชื่อมั่นให้กับลูกค้าและพันธมิตรทางธุรกิจ องค์กรที่มีมาตรการการรักษาความปลอดภัยที่ดีแต่ได้รับความเชื่อถือจากลูกค้าเป็นอย่างมาก นอกจากนี้ ความมั่นคงปลอดภัยทางไซเบอร์ที่เข้มแข็ง จะช่วยลดความเสี่ยงที่อาจจะเกิดขึ้นได้มากยิ่งขึ้น

ข้อสรุปและแนวคิดในการประยุกต์ใช้เพื่อพัฒนาองค์การ

- **การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**
- **การป้องกันความเสี่ยง (Protect) โดยการประเมินช่องโหว่ (Vulnerability Assessment)**
- **การตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)**
- **การเผชิญเหตุภัยคุกคามภัยคุกคามทางไซเบอร์ (Respond) และการฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover)**

“ปัจจัยทั้งหมดข้างต้น เป็นสิ่งที่จะช่วยลดความเสี่ยง และเป็นแนวทางในการป้องกันจากการถูกโจมตีทางไซเบอร์ได้ หากแต่ต้องอาศัยบุคลากรในองค์กรร่วมด้วยช่วยกัน ดำเนินชีวิตประจำวัน ปฏิบัติงานด้วยความระมัดระวังตัวอยู่เสมอ มิเช่นนั้น เราอาจตกเป็นเหยื่อของผู้ไม่หวังดีไม่ทางใดก็ทางหนึ่ง ทั้งจากในองค์กรหรือบุคคล”

แหล่งที่มา

หลักสูตร : หลักสูตรพัฒนาทักษะ ด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

ด้านการพัฒนา (ระบุ ✓) : ☑ ดิจิทัล
☐ ความรู้เฉพาะด้านเพื่อใช้ในการปฏิบัติงาน
☐ เพิ่มศักยภาพตนเอง/ประสิทธิภาพในการทำงาน

บรรยายโดย : ชื่อ-สกุล นายปณิธาน เงินอำนวย ตำแหน่ง ผู้อำนวยการฝ่ายความมั่นคงปลอดภัยทางไซเบอร์
ชื่อ-สกุล นางสาวศรีสุดา แซ่เฮ้ง ตำแหน่ง หัวหน้าทีมแผนและนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์
ชื่อ-สกุล นายคมกริช คำสวัสดิ์ ตำแหน่ง หัวหน้าทีมปฏิบัติการการให้บริการด้านความมั่นคงปลอดภัยทางไซเบอร์
ชื่อ-สกุล นายธงไชย จารุสุรเกษม ตำแหน่ง นักเทคโนโลยีดิจิทัล 2

หน่วยงานผู้รับผิดชอบ : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
วิธีการพัฒนาตนเอง : หลักสูตรออนไลน์ TDGA e-Learning
วันที่ได้รับการฝึกอบรม : 31 กรกฎาคม 2568 **สถานที่ :** กรมพัฒนาที่ดิน