หัวข้อการพัฒนา :

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

สรุปสาระสำคัญ

ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลอื่น โดยไม่ได้รับอนุญาต ปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากมีเป้าหมายและรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น ซึ่งจะสร้างความเสียหายให้กับองค์กรสูงขึ้นเรื่อย ๆ โดยเฉพาะระบบภาครัฐที่เป็นเป้าหมายสำคัญ โดยมีกฎหมายและมาตรฐานที่เกี่ยวข้อง คือ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) มาตรฐานด้านความปลอดภัย ISO 27001 (ระบบบริหารจัดการความปลอดภัยของข้อมูล) ปัจจัยจากบุคลากร (Human Factor) ซึ่ง ความปลอดภัยไม่ได้ขึ้นอยู่กับเทคโนโลยีเพียงอย่างเดียว แต่เกิดจากพฤติกรรมของบุคลากร เช่น การใช้รหัสผ่าน หรือการเปิดอีเมล ซึ่งอาจกลายเป็นภัยคุกคามจากภายในโดยแนวทางแก้ไขคือการสร้างความตระหนักรู้และความเข้าใจในการรักษาข้อมูลให้แก่บุคลากร จะช่วยเปลี่ยนบุคลากรให้เป็นเกราะป้องกันภัยไซเบอร์ และรักษาความน่าเชื่อถือขององค์กร

1. ความรู้พื้นฐานของ Cybersecurity

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยด้านไซเบอร์ มีแนวคิดเสาหลัก 3 ประการ (CIA Model) ประกอบด้วย

1.1 การรักษาความลับของข้อมูล (Confidentiality) คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ เช่น ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้คือ ผู้จัดการทรัพยากรบุคคลเท่านั้น เบอร์โทรของพนักงานในบริษัท จัดเป็นข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

1.2 การรักษาความถูกต้องของข้อมูล (Integrity) คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น ข้อมูลของธนาคารด้านการเงิน ข้อมูลบัญชีธนาคาร ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

1.3 ความพร้อมใช้งานของข้อมูล (Availability) คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น ข้อมูลบัญชีธนาคาร สามรถเรียกดูได้ตลอดระบบฝากถอน ยอดเงิน ที่พร้อมใช้งานสามรถเรียกดูได้ตลอด

2. รูปแบบภัยคุกคามไซเบอร์ (Threat Landscape)

2.1 Malware คือ ซอฟต์แวร์ประเภทหนึ่งที่มีการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อติดตั้งหรือเปิดในระบบ จะทำให้สามารถเข้าถึงระบบคอมพิวเตอร์ได้

2.2 Web-based attacks คือ วิธีการโจมตีโดยผ่านช่องทางเว็บไซต์ โดยการใส่ code ที่ทำให้เมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำไปที่เป้าหมายที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ติด Malware

2.3 Phishing คือ วิธีการโจมตีผ่านทางช่องทางต่าง ๆ เช่น E-Mail /Social โดยใช้วิธีการต่าง ๆ ที่ทำให้หลงเชื่อและให้ข้อมูลส่วนตัว เพื่อนำข้อมูลของเหยื่อไปใช้ในการทำธุรกรรม

2.4 Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ

2.5 Spam คือ วิธีการที่ผู้ไม่ประสงค์ดีทำการส่งข้อมูลผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail, SMS, เป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตเพื่อสร้างความรำคาญ หรือก่อกวน

2.6 DDoS คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ระบบการให้บริการหรือ ระบบเครือข่าย โดยใช้เครื่องโจมตีจำนวนมากยิงมาที่เป้าหมายเดียว เวลาเดียวกัน เพื่อให้เว็บไซต์ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

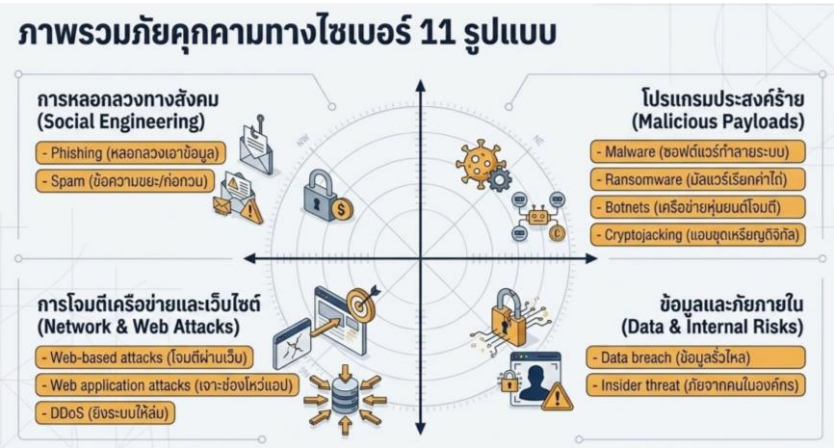
2.7 Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ

2.8 Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ผ่านช่องทางการใช้งานปกติของบุคลากร

2.9 Botnets คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมาย

2.10 Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่าน ที่ใช้ในการปลดล็อคไฟล์

2.11 Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์โดยวิธีการต่าง ๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ



<u>3. ความตระหนักรู้ด้าน Cybersecurity ในการทำงานและชีวิตประจำวัน</u> โดยมีแนวปฏิบัติความปลอดภัยในการทำงานและชีวิตประจำวัน ดังนี้

3.1 การใช้งานอุปกรณ์และระบบการแยกบัญชีผู้ใช้งาน (User) แต่ละบุคคลควรล็อคหน้าจอคอมพิวเตอร์ (Logout) เมื่อไม่อยู่หน้าจอคอมพิวเตอร์ และการตั้งรหัสผ่านที่ปลอดภัย มีความยาวอย่างน้อย 8 ตัวอักษรผสมตัวอักษรเล็ก-ใหญ่ ตัวเลข และอักขระพิเศษ หลีกเลี่ยงคำคาดเดาง่าย เช่น วันเกิด, เลขเรียงกันและเปลี่ยนรหัสผ่านเป็นประจำ

3.2 การจัดการอีเมลและข้อความ การสังเกตและตรวจสอบลิงก์ในอีเมล ไม่คลิกลิงก์หรือดาวน์โหลดไฟล์แนบจากแหล่งที่ไม่น่าเชื่อถือ และหมั่นตรวจสอบผู้ส่ง

3.3 การใช้สื่อสังคมออนไลน์และแอปพลิเคชัน การตรวจสอบบัญชีทางการ (LINE Official, Facebook) ไม่ควรบันทึก password ไว้ที่โปรแกรม และการรู้เท่าทันข่าวปลอม ไม่แชร์ข้อมูลหรือข่าวสารต่าง ๆ ที่ไม่ทราบที่มาของข้อมูล พาดหัวเกินจริง

3.4 บริการคลาวด์และโปรแกรมประชุม กำหนดสิทธิ์เข้าถึงไฟล์เท่าที่จำเป็น และการอัปเดตเวอร์ชันโปรแกรมประชุมออนไลน์อย่างสม่ำเสมอและปิดการแชร์ทันทีเมื่อเลิกใช้งาน

การนำความรู้ไปใช้ประโยชน์

การพัฒนาความรู้เกี่ยวกับการสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) ทำให้ได้รับความรู้และมีความเข้าใจ และตระหนักถึงความสำคัญของความมั่นคงปลอดภัยไซเบอร์ สามารถป้องกันตนเองจากภัยคุกคามไซเบอร์ ตระหนักรู้ถึงเทคนิคการหลอกลวง ทำให้ระมัดระวังการคลิกลิงก์หรือดาวน์โหลดไฟล์แปลกปลอม การปรับเปลี่ยนพฤติกรรมประยุกต์ใช้ในชีวิตประจำวันและการทำงานในองค์กร เพื่อลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ในทุกช่องทาง สามารถปกป้องข้อมูลสำคัญขององค์กรและตนเอง ลดความเสียหายและรักษาความน่าเชื่อถือขององค์กร