การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (Cybersecurity Awareness)

โดย นายสมประสงค์ ประวันนา
นักวิชาการแผนที่ภาพถ่ายปฏิบัติการ

วัตถุประสงค์

๑. เพื่อศึกษาภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
๒. เพื่อศึกษาภัยคุกคามประเภทต่าง ๆ และแนวทางป้องกันแก้ไข

สรุปเนื้อหา

ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ไม่ใช่เพียงเรื่องของเทคโนโลยี แต่เป็นกระบวนการและแนวทางปฏิบัติที่ต้องได้รับความร่วมมือจากบุคลากรทุกระดับ หัวใจสำคัญของความปลอดภัยตั้งอยู่บนหลักการ CIA Triad (Confidentiality, Integrity, Availability) และการรักษาสมดุลระหว่าง ความปลอดภัยและความสะดวกสบาย ในปัจจุบันภัยคุกคามมีความหลากหลายและรุนแรงขึ้น ตั้งแต่ Malware, Phishing ไปจนถึง Inside Threat และ Ransomware องค์กรและบุคคลจึงจำเป็นต้องนำแนวคิด Zero Trust คือ ไม่ไว้วางใจใคร ตรวจสอบทุกครั้ง ให้สิทธิ์น้อยที่สุด และมาตรการป้องกันเชิงรุก เช่น การใช้รหัสผ่านที่ซับซ้อน การเปิดใช้งาน Multi-Factor Authentication (MFA) และการหมั่นอัปเดตซอฟต์แวร์อย่างสม่ำเสมอ มาประยุกต์ใช้อย่างเคร่งครัดเพื่อลดความเสี่ยงและความเสียหายที่อาจเกิดขึ้นความสำคัญขององค์กรดิจิทัล

๑. นิยามและพื้นฐานความมั่นคงปลอดภัยไซเบอร์

๑.๑ Cybersecurity

Cybersecurity คือ การนำเครื่องมือเทคโนโลยี กระบวนการ และวิธีการปฏิบัติมาใช้เพื่อป้องกันและรับมือการโจมตีทางไซเบอร์ที่มุ่งเป้าไปยังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบ หรือโปรแกรม เพื่อป้องกันความเสียหายจากการเข้าถึงโดยไม่ได้รับอนุญาต

๑.๒ กฎหมายและมาตรฐานที่เกี่ยวข้อง

- พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐
- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)
- มาตรฐาน ISO 27001 (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

๑.๓ หลักการ CIA Triad (CIA Model)

เป็นพื้นฐานสำคัญในการปฏิบัติเพื่อความมั่นคงปลอดภัย ประกอบด้วย

C: Confidentiality การรักษาความลับของข้อมูล คือ การกำหนดสิทธิ์เข้าถึงข้อมูลเงินเดือนให้เฉพาะผู้มีส่วนเกี่ยวข้องเท่านั้น

I: Integrity การรักษาความถูกต้องของข้อมูล คือ การป้องกันไม่ให้มีการแก้ไขข้อมูลบัญชีธนาคารโดยไม่ได้รับอนุญาต

A: Availability ความพร้อมใช้งานของข้อมูล คือ ข้อมูลและระบบต้องพร้อมให้เข้าถึงและใช้งานได้ต่อเนื่องตลอดเวลา

๒. รูปแบบภัยคุกคามไซเบอร์ที่สำคัญ

จากการสรุปภัยคุกคามของ ENISA ในปี ๒๐๒๐ รูปแบบการโจมตีที่ควรเฝ้าระวังมีดังนี้

๒.๑ Malware ซอฟต์แวร์ประสงค์ร้าย ได้แก่ Virus, Worms, Trojans ที่ถูกสร้างมาเพื่อส่งผลกระทบต่อระบบและเข้าถึงทรัพยากรเครื่อง

๒.๒ Phishing การหลอกล่อผ่าน E-mail, SMS หรือ Social Media เพื่อให้เหยื่อเผยข้อมูลส่วนตัว เช่น Username และ Password

๒.๓ Ransomware มัลแวร์ที่ทำการเข้ารหัสไฟล์เพื่อล็อคข้อมูลในเครื่องและเรียกค่าไถ่เพื่อแลกกับรหัสปลดล็อค

๒.๔ Data Breach การรั่วไหลของข้อมูลจากการถูกขโมยหรือช่องโหว่ ส่งผลเสียต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

๒.๕ Inside Threat ภัยที่เกิดจากบุคคลภายในองค์กร ทั้งโดยตั้งใจหรือไม่ตั้งใจ ซึ่งมักมีความรุนแรงเนื่องจากภายในมักมีการป้องกันระดับต่ำ

๒.๖ Cryptojacking การแอบใช้ทรัพยากร CPU หรือ GPU ของเครื่องเหยื่อเพื่อประมวลผลเหรียญดิจิทัล (สังเกตได้จาก CPU ทำงาน ๑๐๐% แม้ไม่ได้ใช้งาน)

๒.๗ Distributed Denial of Service (DDoS) การรุมโจมตีจากหลายแหล่งพร้อมกันเพื่อให้ระบบหรือเว็บไซต์ล่มจนใช้งานไม่ได้

๓. แนวทางปฏิบัติเพื่อความปลอดภัยในชีวิตประจำวัน

๓.๑ การจัดการรหัสผ่าน (Password)

- ตั้งรหัสผ่านที่คาดเดายากเป็นด่านหน้าสำคัญของการป้องกัน ควรมีความยาวอย่างน้อย ๘ ตัวอักษร (รหัส ๗ ตัวใช้เวลาแคร็กเพียงไม่กี่มิลลิวินาที ในขณะที่ ๘ ตัวอาจใช้เวลาถึง ๕ ชั่วโมง)
- ความซับซ้อน ใช้ตัวอักษรเล็กใหญ่ ตัวเลข และอักขระพิเศษผสมกัน
- สิ่งที่ควรเลี่ยง คือ ห้ามใช้ Common Password (123456, password) วันเกิด หรือหมายเลขโทรศัพท์
- มาตรการเสริม ควรมีการเปลี่ยนรหัสผ่านสม่ำเสมอ ใช้ Multi-Factor Authentication (MFA) และห้ามใช้รหัสซ้ำกันในแต่ละระบบ

๓.๒ ความปลอดภัยในการใช้งาน E-mail และ Website

- E-mail ไม่เปิดอีเมลหรือไฟล์แนบจากผู้ส่งที่ไม่ชัดเจน ไม่คลิกลิงก์โดยไม่ตรวจสอบ และควรใช้ฟีเจอร์ Report Spam หรือ Report Phishing ใน Gmail
- Website เลือกใช้ Browser มาตรฐาน (Chrome, Firefox) และหมั่นอัปเดตเวอร์ชัน
- การทำธุรกรรมสำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น
- ไม่บันทึกรหัสผ่านบน Browser โดยเฉพาะเมื่อใช้งานเครื่องที่ไม่ใช่เครื่องส่วนตัว ควรใช้โหมด Safe Web Browsing หรือ Incognito
- ติดตั้ง Webcam Cover เพื่อป้องกันการถูกแอบส่องผ่านกล้อง

๓.๓ การใช้งานอุปกรณ์เคลื่อนที่และ IoT

- Mobile: ตั้งค่าล็อกหน้าจอ (PIN, Face scan, Fingerprint) กำหนดสิทธิ์แอปพลิเคชัน (Application Permission) ให้เหมาะสม และไม่อัปโหลดแอปพลิเคชันจากแหล่งที่ไม่รู้จัก

- Internet/IoT เปลี่ยน Default Password ของ Router และอุปกรณ์ IoT ทันทีหลังติดตั้ง เช่น กล้องวงจรปิด และหมั่นอัปเดต Firmware ให้เป็นเวอร์ชันล่าสุดเสมอ

- Free WIFI หลีกเลี่ยงการใช้งาน WiFi ที่ไม่มีรหัสผ่านหรือไม่ทราบที่มาของผู้ให้บริการ

๔. ภัยคุกคามทางสังคม (Fake News)

ข่าวปลอม (Fake News) คือภัยที่สร้างกระแสปลุกปั่นและสร้างความเข้าใจผิดได้อย่างรวดเร็วผ่านช่องทางออนไลน์ วิธีการสังเกตข่าวปลอม เช่น พาดหัวข่าวเกินจริงเพื่อสร้างความน่าสนใจ ระบุที่มาของข่าวไม่ได้หรือไม่มีความน่าเชื่อถือ ไม่ระบุวันและเวลาที่เกิดเหตุการณ์ที่แน่นอน ใช้สำนวนการเขียนในลักษณะการโฆษณาชวนเชื่อ เป็นต้น

๕. มาตรการเชิงบริหารจัดการภายในองค์กร

๕.๑ การจัดการความปลอดภัยสมัยใหม่ (Zero Trust Concept) เป็นการเน้นการตรวจสอบผู้เข้าระบบทุกครั้ง และการให้สิทธิ์เข้าถึง (Access Rights) ที่น้อยที่สุดหรือเท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น

๕.๒ การประชุมออนไลน์ (Conference) ควรใช้สถานที่ที่เหมาะสม มีเฉพาะผู้ที่เกี่ยวข้องเข้าร่วม ระมัดระวังการแชร์เอกสาร และต้องขออนุญาตผู้เข้าร่วมก่อนบันทึกภาพและเสียงทุกครั้ง

๕.๓ Cloud Storage แยก User ใช้งานเป็นรายบุคคล กำหนดสิทธิ์เข้าถึงไฟล์เฉพาะที่จำเป็น และปิดการแชร์ไฟล์ทันทีเมื่อเสร็จสิ้นภารกิจ

การนำองค์ความรู้ไปปรับใช้ในการปฏิบัติงาน

นำความรู้ด้านความมั่นคงทางไซเบอร์ ปฏิบัติตามแนวทางที่กำหนดไว้อย่างเคร่งครัดจะช่วยสร้างเกราะป้องกันที่มีประสิทธิภาพในยุคดิจิทัล เป็นแนวทางการดำเนินงานในยุคดิจิทัล และเพื่อป้องกันการรั่วไหลและความเสียหายที่จะเกิดขึ้นต่อข้อมูลสำคัญในการปฏิบัติงาน

ประโยชน์ที่ได้รับ

- ต่อตนเอง ได้รับองค์ความรู้ในเรื่องความปลอดภัยในการใช้เทคโนโลยี ปรับเปลี่ยนพฤติกรรมการใช้เทคโนโลยีให้มีความปลอดภัย เช่น ตั้งรหัสผ่านแบบ Passphrase เป็นวลียาว ๆ ที่จำง่ายแต่เดายากแทนรหัสผ่านสั้น ๆ เปิดใช้งาน Multi-Factor Authentication (MFA) ในทุกระบบที่รองรับ เพื่อป้องกันการถูกสวมรอยแม้รหัสผ่านจะหลุดไป เช็กชื่อผู้ส่ง (Sender Address) ให้ละเอียดก่อนคลิก เพื่อป้องกัน Phishing เป็นต้น

- ต่อองค์กร นำหลักด้านความมั่นคงทางไซเบอร์มาปรับปรุงวิธีการทำงานให้สอดคล้องกับหลัก CIA Triad และ PDPA เพื่อใช้ในองค์กร จะช่วยให้ข้อมูลขององค์กรมีความมั่นคงปลอดภัย ข้อมูลจะไม่มีการรั่วไหลและสูญหาย เช่น การจัดการสิทธิ์ (Least Privilege) ในการแชร์ไฟล์ผ่าน Cloud Storage เช่น Google Drive, OneDrive ให้กำหนดสิทธิ์เฉพาะ ผู้ที่เกี่ยวข้อง และตั้งค่าเป็น Viewer หรือ Commenter แทนการให้สิทธิ์ Editor แก่ทุกคน และปิดการแชร์ทันทีเมื่อจบโครงการหรือภารกิจ ในการประชุมออนไลน์ Secure Conferencing ต้องมีการตั้งรหัสผ่าน (Meeting Password) หรือมีระบบ Waiting Room เพื่อคัดกรองคนเข้าประชุม และระมัดระวังการ Share Screen ไม่ให้ติดข้อมูลส่วนบุคคลหรือหน้าต่างแอปพลิเคชันอื่นที่ไม่เกี่ยวข้อง เป็นต้น

- ต่อสาธารณะ เมื่อเจ้าหน้าที่ในองค์กรมีความรู้ ข้อมูลที่เก็บมาจากประชาชนที่เป็นข้อมูลสาธารณะจะมีความปลอดภัยไม่เกิดการรั่วไหล

แหล่งที่มา

หลักสูตร : การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (Cybersecurity Awareness)
บรรยายโดย : คุณพลากร ลาภอลงกรณ์ ผู้จัดการส่วนบริการลูกค้า ฝ่ายปฏิบัติการ
สถาบัน/หน่วยงาน/ระบบ : สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
รูปแบบหลักสูตร : หลักสูตรออนไลน์ TDGA E-Learning
ช่วงเวลาการฝึกอบรม : ตุลาคม ๒๕๖๘ - มีนาคม ๒๕๖๙