

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)

โดย นายเนติพงศ์ ศรีสว่าง
นักวิชาการแผนกที่ภาพถ่ายปฏิบัติการ

วัตถุประสงค์

- เพื่อสร้างความเข้าใจในพื้นฐานและนิยามของความมั่นคงปลอดภัยไซเบอร์
- เพื่อเรียนรู้มาตรฐานและหลักการสากลในการปกป้องข้อมูล
- เพื่อให้ผู้เข้าทำนรูปแบบภัยคุกคามที่มีความหลากหลายและสร้างทักษะการป้องกันตนเองและสร้าง "ความตระหนักรู้" (Awareness) ในการป้องกันภัยคุกคาม
- เพื่อเสริมสร้างวินัยในการใช้งานเทคโนโลยีสารสนเทศ

สรุปเนื้อหา

นิยามและขอบเขตของ Cybersecurity

Cybersecurity (ความมั่นคงปลอดภัยไซเบอร์) หมายถึง การประยุกต์ใช้เทคโนโลยี กระบวนการจัดการ และการควบคุมความเสี่ยง เพื่อปกป้องระบบคอมพิวเตอร์ เครือข่าย อุปกรณ์ และข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาต หรือการโจมตีทางดิจิทัลที่มุ่งเป้าทำลาย เปลี่ยนแปลง หรือขโมยข้อมูลสำคัญ ในปัจจุบันหน่วยงานทั้งภาครัฐและเอกชนต่างให้ความสำคัญอย่างยิ่งเนื่องจากรูปแบบการโจมตีมีความซับซ้อนมากขึ้น และสามารถสร้างความเสียหายต่อทรัพย์สินและชื่อเสียงขององค์กรได้อย่างมหาศาล

โครงสร้างและมาตรฐานความมั่นคงปลอดภัยพื้นฐาน

เพื่อให้เกิดความมั่นคงปลอดภัยที่เป็นระบบ จึงมีการกำหนดกฎหมายและมาตรฐานสากล รวมถึงหลักการสำคัญที่เป็นหัวใจหลัก ดังนี้

- กฎหมายสำคัญในประเทศไทย
 - พ.ร.บ. ไซเบอร์ฯ (๒๕๖๒) เน้นการป้องกันภัยระดับโครงสร้างพื้นฐานของประเทศ
 - พ.ร.บ. คอมพิวเตอร์ฯ (๒๕๖๐) เน้นการลงโทษผู้กระทำความผิดทางดิจิทัล
 - พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) เน้นสิทธิและความเป็นส่วนตัวของเจ้าของข้อมูล
 - มาตรฐานสากล: ISO ๒๗๐๐๑ ซึ่งเป็นมาตรฐานสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS)
- หลักการ CIA Triad ประกอบด้วย
 - Confidentiality (การรักษาความลับ) การเข้าถึงข้อมูลต้องถูกจำกัดไว้เฉพาะผู้ที่มีสิทธิ์ตามระดับความสำคัญ เช่น ข้อมูลเงินเดือน (ลับมาก) หรือข้อมูลภายในบริษัท
 - Integrity (การรักษาความถูกต้อง) การรับประกันว่าข้อมูลจะไม่ถูกแก้ไขหรือเปลี่ยนแปลงระหว่างทางหรือจากผู้ไม่มีสิทธิ์ เช่น ยอดเงินในบัญชีธนาคาร
 - Availability (ความพร้อมใช้งาน) ข้อมูลและระบบต้องพร้อมใช้งานเสมอเมื่อต้องการ โดยเฉพาะระบบสำคัญอย่าง Server หรือระบบการเงิน

การจำแนกรูปแบบภัยคุกคามทางไซเบอร์ (Cyber Threats) ภัยคุกคามสามารถแบ่งออกเป็นหลายประเภทตามวิธีการและเป้าหมายของผู้โจมตี

- กลุ่มซอฟต์แวร์อันตราย (Malware): ครอบคลุมทั้ง Virus (ฝังตัวกับโปรแกรม), Worms (แพร่กระจายเองได้), Trojans (หลอกว่าเป็นโปรแกรมดี) และ Ransomware (มัลแวร์เรียกค่าไถ่ที่ทำการเข้ารหัสไฟล์เพื่อลิดลอกข้อมูล)

๒. การโจมตีผ่านเครือข่ายและเว็บ

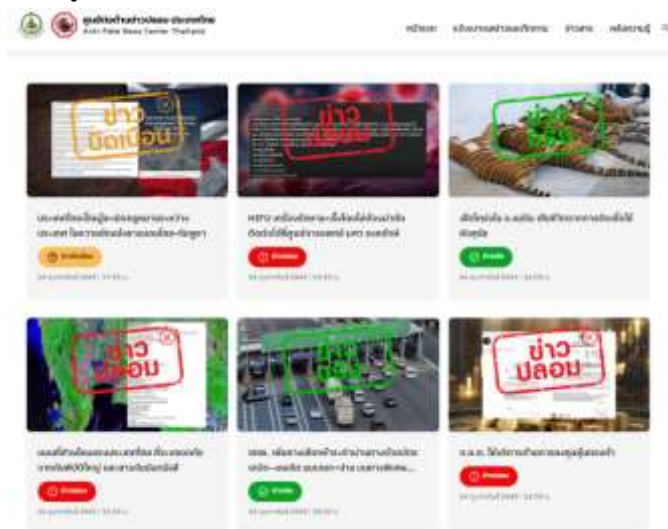
- ๑) Web-based attacks การฝัง Code อันตรายในเว็บไซต์ที่มีช่องโหว่
- ๒) Web application attacks เช่น SQL Injection หรือ Cross-Site Scripting (XSS)
- ๓) DDoS การระดมยิงข้อมูลเพื่อให้ระบบล่มจนใช้งานไม่ได้

๓. การหลอกลวงทางสังคมและข้อมูล

- ๑) Phishing การปลอมแปลงอีเมลหรือข้อความเพื่อขโมยรหัสผ่าน
- ๒) Spam การส่งข้อมูลขยะก่อกวนจำนวนมาก
- ๓) Fake News ข่าวปลอมที่มุ่งเน้นการสร้างกระแสและปลุกปั่น โดยมักมีพาดหัวเกินจริง

และไม่ระบุที่มา

๔. ภัยด้านเทคนิคอื่น ๆ Data Breach (ข้อมูลรั่วไหล), Insider Threat (ภัยจากคนใน), Botnets (เครือข่ายหุ่นยนต์ที่ถูกสั่งการโจมตี) และ Cryptojacking (แอบใช้เครื่องเหยื่อขุดเหรียญดิจิทัล)



ภาพที่ ๑ ตัวอย่างการตรวจสอบข่าวปลอมของศูนย์ต่อต้านข่าวปลอมประเทศไทย

(ที่มา : ภาพประกอบโดยศูนย์ต่อต้านข่าวปลอมประเทศไทย, ณ วันที่ ๒๔ กุมภาพันธ์ ๒๕๖๙

<https://www.antifakenewscenter.com/tag/ศูนย์ต่อต้านข่าวปลอม/>)

แนวทางสร้างความตระหนักรู้และการป้องกันในชีวิตประจำวัน

การป้องกันที่ดีที่สุดเริ่มต้นที่ "ผู้ใช้งาน" ผ่านแนวทางปฏิบัติตามมาตรฐานความปลอดภัย ดังนี้

๑. การจัดการรหัสผ่านที่ดี (Strong Password)

- ๑) มีความยาวอย่างน้อย ๘ ตัวอักษร ผสมอักขระพิเศษ ตัวเลข และตัวอักษรพิมพ์

ใหญ่-เล็ก

- ๒) หลีกเลี่ยงรหัสที่เดาง่าย เช่น "๑๒๓๔๕๖" หรือวันเกิด

- ๓) เปิดใช้งานการยืนยันตัวตนแบบหลายชั้น (Multi-Factor Authentication - MFA)

๒. สำหรับอุปกรณ์

- ๑) อัปเดตระบบปฏิบัติการ (OS) และ Patch ความปลอดภัยอย่างสม่ำเสมอ

- ๒) ติดตั้งและอัปเดต Anti-Malware เสมอ

- ๓) ไม่บันทึกหรือส่งผ่านไว้ใน Browser หรือจดติดไว้ในหน้าจอคอมพิวเตอร์

๓. การใช้งานอินเทอร์เน็ตและสื่อสาร

- ๑) E-mail ไม่เปิดไฟล์หรือคลิกลิงก์ที่น่าสงสัย

- ๒) Wi-Fi หลีกเลี่ยง Free Wi-Fi ที่ไม่รู้ที่มาหรือไม่ใส่รหัสผ่าน

๓) Mobile ดาวน์โหลดแอปพลิเคชัน จาก Store ทางร้านที่นั่น และตรวจสอบสิทธิ์การเข้าถึง (Permission) ของแอปพลิเคชัน ให้เหมาะสม

๔) การทำงานและการประชุมออนไลน์: เลือกสถานที่ที่เหมาะสม รมั้ดระวังการแชร์หน้าจอ และขออนุญาตผู้เข้าร่วมก่อนบันทึกภาพ/เสียงเสมอ

การนำองค์ความรู้ไปปรับใช้ในการปฏิบัติงาน

- การจัดการอัตลักษณ์ ใช้รหัสผ่านที่ซับซ้อนและแตกต่างกันในแต่ละระบบ และเปิดใช้งาน Multi-Factor Authentication (MFA) ทุกครั้งที่ทำได้ เพื่อป้องกันการสวมรอย

- การสำรองข้อมูล (Availability) ทำการสำรองข้อมูลสำคัญอย่างสม่ำเสมอและแยกเก็บไว้ในที่ปลอดภัย เพื่อให้มั่นใจว่าหากเกิดเหตุการณ์ระบบล่มหรือโดน Ransomware งานจะสามารถดำเนินต่อไปได้

- ความตระหนักรู้ต่อสื่อ ตรวจสอบซีอีเมลผู้ส่งอย่างละเอียดก่อนคลิกลิงก์หรือโหลดไฟล์แนบ เพื่อป้องกันภัยจาก Phishing และ Ransomware

- การประชุมออนไลน์ ใช้โปรแกรมที่มาตรฐานกำหนด ตั้งรหัสผ่านห้องประชุม และตรวจสอบรายชื่อผู้เข้าร่วมก่อนเริ่มนำเสนอข้อมูลสำคัญ

- การทำงานนอกสถานที่ หลีกเลี่ยงการใช้ Free Wi-Fi ในการเข้าถึงระบบภายในบริษัท หากจำเป็นควรใช้ VPN หรือ Hotspot ส่วนตัวเพื่อความปลอดภัย

- การคัดกรองข่าวสาร ก่อนแชร์ข้อมูลภายในหรือข่าวสารใด ๆ ต้องตรวจสอบแหล่งที่มาเพื่อป้องกันการแพร่กระจาย Fake News ที่อาจส่งผลกระทบต่อชื่อเสียงหรือการตัดสินใจขององค์กร

ประโยชน์ที่ได้รับ

๑. ต่อตนเอง

๑) สร้างความมั่นใจในการทำงาน การมีความรู้ด้านดิจิทัล (Digital Literacy & Security) ช่วยให้สามารถใช้งานระบบได้อย่างมั่นใจและปลอดภัย

๒) ปกป้องข้อมูลส่วนบุคคล ช่วยให้รู้วิธีแยกแยะระหว่างข้อมูลส่วนตัวและข้อมูลทางราชการ ป้องกันการถูกโจรกรรมข้อมูลส่วนตัว (Identity Theft) จากมิจฉาชีพที่มักแอบอ้างหน่วยงานรัฐ

๓) ลดความวิตกกังวล เมื่อรู้วิธีป้องกันและรับมือที่ถูกต้อง จะช่วยให้ใช้งานเทคโนโลยีได้อย่างมั่นใจ ไม่ตื่นตระหนกต่อข่าวลือหรือภัยคุกคามใหม่ ๆ

๒. ต่อองค์กร

๑) รักษาความมั่นคงปลอดภัยของข้อมูลภาครัฐ ป้องกันการรั่วไหลของข้อมูลชั้นความลับของทางราชการ และข้อมูลทะเบียนราษฎร์ต่าง ๆ ตามหลัก Confidentiality

๒) ความต่อเนื่องในการบริการประชาชน เมื่อระบบปลอดภัยจากมัลแวร์หรือการโจมตีแบบ DDoS หน่วยงานจะสามารถให้บริการประชาชนได้อย่างต่อเนื่อง (Availability) เช่น ระบบการลงทะเบียน หรือระบบรับคำร้องออนไลน์ไม่ล่ม

๓) ประหยัดงบประมาณแผ่นดิน การป้องกันเชิงรุกช่วยลดค่าใช้จ่ายในการกู้คืนระบบหรือค่าปรับที่อาจเกิดขึ้นหากมีการละเมิดข้อมูลส่วนบุคคล (PDPA) รวมถึงลดความเสียหายต่อทรัพย์สินทางราชการ

๓. ต่อสาธารณะ

๑) ลดปัญหาอาชญากรรมทางเทคโนโลยี การรู้เท่าทัน Fake News และการหลอกลวงออนไลน์ ช่วยลดจำนวนเหยื่อในสังคม และลดภาระของเจ้าหน้าที่บ้านเมืองในการปราบปราม

๒) ประชาชนที่มามีติดต่อราชการมีความมั่นใจว่าข้อมูลชื่อ ที่อยู่ เลขบัตรประชาชน หรือข้อมูลทางการเงินของตนมีความปลอดภัย

๓. ยุกระดับรัฐบาลดิจิทัล (Digital Government) เป็นรากฐานสำคัญในการขับเคลื่อนนโยบายเศรษฐกิจดิจิทัล ทำให้ประเทศไทยมีความน่าเชื่อถือในสายตาของนักลงทุนและนานาชาติ

แหล่งที่มา

หลักสูตร : การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)

บรรยายโดย : คุณพลากร ลาภอลงกรณ์

สถาบัน/หน่วยงาน/ระบบ : TDGA

รูปแบบหลักสูตร : การเรียนรู้ออนไลน์ TDGA e-Learning

ช่วงเวลาการฝึกอบรม : กุมภาพันธ์ ๒๕๖๙