การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

โดย นายอนุพงษ์ จันทร์เพ็งเพ็ญ
นายช่างสำรวจชำนาญงาน

วัตถุประสงค์

๑. เพื่อให้ผู้เรียนมีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน

๒. เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับรูปแบบภัยคุกคามประเภทต่าง ๆ และแนวทางป้องกันแก้ไข

๓. เพื่อให้ผู้เรียนสามารถนำความรู้ไปประยุกต์ใช้ในการทำงาน และชีวิตประจำวันได้อย่างถูกต้อง

สรุปเนื้อหา

๑. Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กร เพิ่มมากขึ้นเรื่อย ๆ

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

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

๒. ความรู้พื้นฐานของ Cybersecurity พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ CIA Triad หรือ CIA Model ซึ่งประกอบด้วยตัวซี (C) ตัวไอ (I) และตัวเอ (A)

C: Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น
- เบอร์โทรของพนักงานในบริษัท จัดเป็นข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

I: Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

A: Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

๓. รูปแบบภัยคุกคามของ Cybersecurity

๑) Malware คือ ซอฟต์แวร์ หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึงไวรัส (Virus) เวิร์ม (Worms) โทรจัน (Trojans)

๒) Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ Code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

เว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไข Code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System)

๓) Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่าง ๆ เช่น E-Mail SMS เว็บไซต์ หรือช่องทาง Social โดยใช้วิธีหลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username Password หรือข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

๔) Web application attack คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น

- Code ของเว็บไซต์ เช่น CMS
- Web Server หรือ Database Server

วิธีการโจมตีที่นิยมใช้

- Cross-Site Scripting
- SQL injection
- Path Traversal

๕) Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล ข้อความ หรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail SMS เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญหรือก่อกวน

๖) DDos (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์ ระบบการให้บริการ ระบบเครือข่าย ไม่สามารถใช้งานได้หรือระบบล่ม

๗) Data Breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขายหรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ โดยผลกระทบ เช่น

- ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่
- ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
- สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

๘) Inside threat คือ ภัยที่เกิดจากภายในบุคลากรภายในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือสมาร์ตโฟน เป็นต้น ซึ่ง Inside threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กรอาจจะมีการป้องกันในระดับต่ำทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

วิธีการป้องกัน

นำหลักการ Zero Trust มาใช้ภายในองค์กร ซึ่ง Zero Trust เป็นคอนเซปต์การจัดการซีเคียวริตี้สมัยใหม่ที่หลายองค์กรได้นำมาปรับใช้ ตั้งแต่การตรวจสอบผู้เข้าระบบทุกครั้ง การให้สิทธิ์ที่น้อยที่สุด หรือเท่าที่จำเป็นกับผู้ใช้งาน

๙) Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมาย หรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๑๐) Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อกไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อกไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อกไฟล์ เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน

- สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล
- ควรติดตั้ง Anti-malware และมีการ Update อย่างสม่ำเสมอ
- ก่อนเปิดไฟล์ต่าง ๆ ที่ได้รับมา ควรมีความตระหนักก่อนที่จะทำการเปิด

๑๑) Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่าง ๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวณผลเพื่อสร้างรายได้กลับไปที่ Hacker

๔. ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยในการใช้งาน มีดังนี้

การใช้งาน Computer

๑. ควรมีการแยก user ใช้งานกันของแต่ละบุคคล ๒. ควร logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์ ๓. ควรติดตั้ง Anti-malware และมีการ Update อย่างสม่ำเสมอ ๔. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ ๕. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ ๖. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ ๗. มีการใช้ Password ที่ดีและไม่ควรบอก Password แก่ผู้อื่น

การใช้ Password

๑. ความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (# @ $!) ๒. ควรให้มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร ๓. ควรหลีกเลี่ยงการใช้ Common Password หรือ Default Password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น Password 123456 วันเกิด หมายเลขโทรศัพท์ ๔. ควรมีการเปลี่ยน Password อย่างสม่ำเสมอ ๕. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ ๖. ควรใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้ ๗. ไม่ควรบอก Password แก่ผู้อื่นโดยไม่จำเป็น

การใช้ E-mail

๑. ไม่ควรเปิด E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน ๒. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน ๓. อย่าคลิก Link ใน E-mail โดยไม่มีการตรวจเช็ค ๔. ในเรื่องที่มีความสำคัญก่อนทำธุรกรรมใด ๆ ควรมีการเช็คผ่านทางช่องทางอื่น ๆ เพิ่มเติม

การใช้งาน Website

๑. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่าง ๆ ๒. ไม่ควรทำการบันทึก Password ต่าง ๆ บน Browser ๓. ควรมีการ Update Browser ให้เป็น Version ล่าสุด ๔. ติดตั้ง Anti-malware แล้วทำการ Update อย่างสม่ำเสมอ ๕. เว็บไซต์สำหรับการทำธุรกรรมที่สำคัญหรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น ๖. ในกรณีที่เครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing ๗. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งานกัน เช่น Google chrome, Mozilla Firefox เป็นต้น

การใช้ Messaging

๑. ไม่ควรบันทึก Password ไว้ที่โปรแกรม ๒. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัวไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง ๓. ต้องมีความตระหนักก่อนเปิด Link หรือไฟล์ต่าง ๆ ที่ได้รับมา ๔. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ ๕. ไม่ควรแชร์ข้อมูลหรือข่าวสารต่าง ๆ โดยไม่ทราบที่มาของข้อมูล

Fake News หรือ ข่าวปลอม เป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือจึงทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแสปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ทางช่องทางออนไลน์ เช่น LINE Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น

วิธีการสังเกตข่าวปลอม ๑. มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ ๒. ระบุที่มาของข่าวไม่ได้ ๓. มักจะไม่ระบุวันที่และเวลาที่เกิดเหตุการณ์ ๔. สำนวนการเขียนออกแนวการโฆษณา

การใช้ Conference

๑. ใช้สถานที่เหมาะสมกับการ Conference ๒. ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง ๓. แชร์เอกสารต่าง ๆ อย่างระมัดระวัง ๔. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน ๕. มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ ๖. ควรมีการขออนุญาตผู้เข้าร่วมประชุม Conference ก่อนที่จะบันทึกภาพและเสียง

การใช้ Cloud Storage

๑. แยก User ในการใช้งานของแต่ละบุคคล ๒. ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น ๓. ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น ๔. Update Version ของโปรแกรมอย่างสม่ำเสมอ ๕. ติดตั้ง Anti-malware และ Update อย่างสม่ำเสมอ ๖. ตั้ง Password ที่ดีและไม่บอก Password แก่ผู้อื่น

การใช้ Mobile

๑. เปิดการใช้งาน PIN/Password Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์ ๒. ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา ๓. กำหนด Application permission ให้เหมาะสม ๔. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างเหมาะสม ๕. Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

การใช้ Internet Connection

๑. เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน ๒. เปลี่ยน SSID และรหัสผ่านของ Wi-Fi ที่กำหนดมาจากผู้ให้บริการ ๓. กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น

การใช้ IoT Devices

๑. เปลี่ยน Default Password ที่มาจากโรงงาน ๒. ควรมีการ Update Firmware ให้เป็น Version ล่าสุด ๓. ใช้ Application ที่ใช้ในการคอนโทรลกับอุปกรณ์ต่าง ๆ ให้เป็น Version ล่าสุด

IoT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่าย Internet เพื่อใช้ในการทำงานร่วมกับระบบต่าง ๆ หรือ Application ต่าง ๆ ได้ เช่น หลอดไฟ พัดลม เครื่องกรองอากาศ ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว

การนำองค์ความรู้ไปปรับใช้ในการปฏิบัติงาน

สามารถนำองค์ความรู้การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งไม่ได้เป็นเพียงเรื่องของฝ่ายไอทีเท่านั้น มาใช้เพื่อลดและป้องกันความเสี่ยงจากภัยคุกคามไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงานได้

ประโยชน์ที่ได้รับ

- ต่อตนเอง เสริมสร้างวินัยและนิสัยที่ดีในการปฏิบัติงานทำให้มีความรู้ความเข้าใจเกี่ยวกับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์มากยิ่งขึ้น

- ต่อองค์กร สามารถนำความรู้ที่ได้รับมาประยุกต์ใช้ในการปฏิบัติงานได้อย่างถูกต้อง

- ต่อสาธารณะ สร้างภูมิคุ้มกันดิจิทัลให้กับสังคมช่วยให้ประชาชนรู้จักวิธีจัดการข้อมูลที่ละเอียดอ่อน เช่น ข้อมูลทางการเงิน ข้อมูลส่วนตัวและที่อยู่ ป้องกันการรั่วไหลที่นำไปสู่ความเสียหายต่อทรัพย์สินช่วยลดโอกาสการตกเป็นเหยื่อทางไซเบอร์

แหล่งที่มา

หลักสูตร : การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)
บรรยายโดย : นายพลากร ลาภอลงกรณ์
สถาบัน/หน่วยงาน/ระบบ : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
รูปแบบหลักสูตร : การเรียนรู้ออนไลน์ TDGA e-Learning
ช่วงเวลาฝึกอบรม : กุมภาพันธ์ ๒๕๖๙