แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต ๒
รอบการประเมินที่ ๒/๒๕๖๗ ตั้งแต่วันที่ ๑ เมษายน ๒๕๖๗ – ๓๐ กันยายน ๒๕๖๗
ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

ชื่อ-นามสกุล นางนารินทร์ อุบลนุช **ตำแหน่ง** นักวิชาการเกษตรชำนาญการ

หน่วยงาน สถานีพัฒนาที่ดินระยอง

หัวข้อการพัฒนา การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness

วิธีการพัฒนา ฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ออนไลน์

วันที่พัฒนา ๑๖ สิงหาคม ๒๕๖๗ **สถานที่** สถานีพัฒนาที่ดินระยอง

หน่วยงานที่จัดอบรม สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัลTDGA (Thailand digital government academy)

วัตถุประสงค์

๑. เพื่อให้ผู้เรียนมีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
๒. เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับภัยคุกคามประเภทต่างๆ และแนวทางป้องกันแก้ไข
๓. เพื่อให้ผู้เรียนสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

สรุปสาระสำคัญ

ความหมายของ Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์

การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายัง อุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรม ที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานรัฐและบริษัทเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีและรูปแบบ การโจมตีทางด้านไซเบอร์มีความหลากหมายมากขึ้น และสร้างความเสียหายให้กับองค์กรมากขึ้น

ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

๒.๑ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
๒.๒ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับอมพิวเตอร์ พ.ศ. ๒๕๖๐
๒.๓ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
๒.๔ มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ “CIA Triad”

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ CIA Triad หรือ CIA Model ซึ่งประกอบด้วยตัวซี(C) ตัวไอ(I) และตัวเอ(A)

C:Confidentiality หรือ การรักษาความลับของข้อมูล คือ การรักษาความลับของข้อมูล คือการที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น - ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการ ส่วนทรัพยากรบุคคลเท่านั้น

I:Integrity หรือ การรักษาความถูกต้องของข้อมูล คือการที่ระบบสิทธิของการแก้ไขข้อมูล และการ รักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น ข้อมูลของธนาคารด้านการเงิน ข้อมูลบัญชีธนาคาร ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

A:Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร

- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์ **สรุปคือ CIA Model** สามารถนำมาปรับใช้ให้เข้ากับส่วนของข้อมูลที่อยู่บนระบบคอมพิวเตอร์ได้

รูปแบบภัยคุกคามของ Cybersecurity

ในภาพ คือตัวอย่างจาก ENISA คือ องค์กรของฝั่งยุโรปที่ดูแลเรื่องภัยคุกคามทางไซเบอร์ สรุป ๑๕ ภัยคุกคามที่ เกิดขึ้นในปี ๒๐๒๐ ดังนี้

Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึงไวรัส (Virus) เวิร์ม (Worms) โทรจัน (Trojans)

Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ Code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไป ที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware เพิ่มเติม : เว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไข Code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System)

Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่าง ๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username Password หรือ ข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

Web application attack คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆเช่น Code ของเว็บไซต์ เช่น CMS Web Server หรือ Database Server วิธีการโจมตีที่นิยมใช้ Cross-Site Scripting, SQL injection, Path Traversal สามารถศึกษาวิธีการป้องกันเพิ่มเติมได้จากมาตรฐาน OWASP Top Ten

Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail SMS เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาต ไปยังผู้รับเพื่อสร้างความรำคาญหรือก่อกวน

DDos (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ ระบบการให้บริการ หรือ ระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์ ระบบการให้บริการ ระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

Data Breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ ข้อมูลของแอปพลิเคชั่น หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชั่น หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ ผลกระทบสร้างความเสียหายข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่ ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล ตลอดจนสร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

Inside threat คือ ภัยที่เกิดจากภายในบุคลากรภายในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น

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

Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ และก่อนเปิดไฟล์ต่าง ๆ ที่ได้รับมา ควรมีความตระหนักก่อนที่จะทำการเปิดหากไม่มั่นใจไม่ควรเปิดไฟล์

ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน แบ่ง ๒ ช่วงเวลาคือ ช่วงทำงาน ช่วงวันพักผ่อน ช่วงเวลาทำงานควรตระหนักรู้ดังนี้

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยของ Computer

ควรมีการแยก user ใช้งานกันของแต่ละบุคคล ควร logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์ ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ มีการอัพเดท Patch หรืออัพเดต window ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ ไม่ควรจด password และติด password ไว้ที่หน้าจอ มีการใช้ password ที่ดีและไม่ควรบอก password แก่ผู้อื่น

Password การใช้ Password ที่ดี คือ

มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น password ๑๒๓๔๕๖ วันเกิด หมายเลขโทรศัพท์ ควรมีการเปลี่ยน Password อย่างสม่ำเสมอ หากใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้ ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบและไม่ควรบอก Password แก่ผู้อื่น

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย E-mail

ไม่เปิด E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน ไม่คลิกลิงก์ใน E-mail โดยไม่มีการตรวจเช็ค และเรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการเช็คผ่านทางช่องทางอื่น ๆ เพิ่มเติม

Website สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง social ต่างๆ ไม่ควรทำการบันทึก Password ต่างๆบน Browser เว็บไซต์สำหรับการทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งาน ผ่าน HTTPS เท่านั้น ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งานเช่น google chrome mozilla firefox เป็นต้น ควรมีการอัพเดทเวอร์ชั่นของ Browser อย่างสม่ำเสมอ ในกรณีที่เครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน browser ในโหมด safe web browsing และควรติดตั้ง anti-malware และ update อย่างสม่ำเสมอ

Fake News Fake News หรือ ข่าวปลอม ไม่ควรแชร์ส่งต่อ

เป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวปลอม ที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือจึงทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแสปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ทางช่องทางออนไลน์ เช่น LINE Facebook ทำให้มีการกระจายข่าว ได้อย่างรวดเร็วมากยิ่งขึ้น

วิธีการสังเกตข่าวปลอม

มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ ระบุที่มาของข่าวไม่ได้ มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์ สำนวนการเขียนออกแนวการโฆษณาชวนเชื่อทำให้ผู้อ่านสะดุดตาให้สนใจเข้าไปอ่าน

รูปแบบบัญชีของLine Line Official Account ชนิดของบัญชี Line Official Account ที่ปลอดภัย

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย Conference

ใช้สถานที่เหมาะสมกับการ Conference ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง แชร์เอกสารต่าง ๆ อย่างระมัดระวัง ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน มีการอัพเดทเวอร์ชั่นของโปรแกรม Conference อย่างสม่ำเสมอ เพิ่มเติม : ควรมีการขออนุญาตผู้เข้าร่วมประชุม Conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม

Cloud Storage สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

ควรแยก User ในการใช้งานของแต่ละบุคคล มีการกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น ควรติดตั้ง anti-malware และ update อย่างสม่ำเสมอ มีการอัพเดทเวอร์ชั่นของโปรแกรมอย่างสม่ำเสมอ และมีการตั้ง Password ที่ดีและไม่บอก Password แก่ผู้อื่น

Computer สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

ควรมีการแยก User ใช้งานกันของแต่ละบุคคล มีการ Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์ ควรติดตั้ง anti-malware และมีการอัพเดตอย่างสม่ำเสมอ มีการอัพเดท Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ มีการอัพเดทเวอร์ชั่นของโปรแกรมบนเครื่องอย่างสม่ำเสมอ ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ และไม่ควรบอก Password แก่ผู้อื่น

Free WIFI สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

ไม่ควรใช้งาน WiFi ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน หลีกเลี่ยงการใช้งาน WiFi ที่ไม่รู้ที่มาในการให้บริการ

Mobile สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

เปิดการใช้งาน PIN/Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์ ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา กำหนด Application permission ให้เหมาะสม มีการอัพเดท Patch ระบบปฏิบัติการ (OS) อย่างเหมาะสม มีการอัพเดทเวอร์ชั่นของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

Internet Connection สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน เปลี่ยน SSID และรหัสผ่านของ WiFi ที่กำหนดมาจากผู้ให้บริการ กำหนดผู้ที่สามารถเข้าใช้งานอินเทอร์เน็ตเท่าที่จำเป็น

IoT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต

เพื่อใช้ในการทำงานร่วมกับระบบต่าง ๆ หรือ Application ต่าง ๆ ได้ เช่น หลอดไฟ พัดลม เครื่องกรองอากาศ ซึ่งเมื่อสามารถ ต่อกับเครือข่ายได้ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย เปลี่ยน Default Password ที่มาจากโรงงาน ควรมีการอัพเดทเฟิร์มแวร์ให้เป็นเวอร์ชั่นล่าสุด ใช้ application ที่ใช้ในการคอนโทรลกับอุปกรณ์ต่าง ๆ ให้เป็นเวอร์ชั่นล่าสุด กล้องวงจรปิดที่ดูผ่านอินเตอร์เน็ตควรมีการเปลี่ยน password ที่ไม่ใช่ default password จากโรงงาน เพื่อป้องกันความปลอดภัยความเป็นส่วนตัว

ประโยชน์ที่ได้รับจากการพัฒนาความรู้

สร้างความตระหนักรู้ ความมั่นคงทางไซเบอร์ เพื่อความปลอดภัยในชีวิตประจำวัน ไซเบอร์มีความสะดวกรวดเร็วต่อชีวิตประจำวันทำให้รู้เท่าทันการใช้อิเล็กทรอนิค รู้ถึงการคุกคามไซเบอร์ในรูปแบบต่างๆใช้ชีวิตอย่างมั่นคงและปลอดภัยมากยิ่งขึ้น

(นางนารินทร์ อุบลนุช)
นักวิชาการเกษตรชำนาญการ

(นายศราวุธ ศิริลักณ์)
ผู้อำนวยการสถานีพัฒนาที่ดินระยอง