สรุปบทเรียนการพัฒนาความรู้
หลักสูตร “การสร้างความตระหนักรู้ความมั่นคงทางไซเบอร์ (Cyber Security Awareness)”

****

ชื่อ-สกุล: นางอัจจิมา พงษ์จินดา **ตำแหน่ง:** นักวิทยาศาสตร์ชำนาญการ
สังกัด: กลุ่มวิจัยเคมีดิน สำนักวิทยาศาสตร์เพื่อการพัฒนาที่ดิน กรมพัฒนาที่ดิน
วันที่อบรม: 8 พฤษภาคม 2568

วัตถุประสงค์ของหลักสูตร

1. เพื่อให้มีความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในปัจจุบัน
2. เพื่อให้มีความรู้เกี่ยวกับภัยคุกคามประเภทต่าง ๆ และแนวทางแก้ไข
3. เพื่อให้สามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

สรุปบทเรียน

ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์ก็มีความหลากหลายมากขึ้นด้วย และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อย ๆ ดังนั้น ความรู้พื้นฐานของ Cybersecurity จึงมีความจำเป็นต่อความตระหนักรู้สู่การนำไปประยุกต์ใช้ในการทำงานและการใช้ชีวิตประจำวัน

1. ความรู้พื้นฐานของ Cybersecurity

ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ที่เรียกว่า CIA Triad หรือ CIA Model สามารถนำมาปรับใช้ให้เข้ากับส่วนของข้อมูลที่อยู่บนระบบคอมพิวเตอร์ได้ ประกอบด้วยตัวซี (C) ตัวไอ (I) และตัวเอ (A) ซึ่งมีรายละเอียด ดังนี้

C: Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ เช่น ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น หรือ เบอร์โทรศัพท์ของพนักงานในบริษัท จัดเป็นข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน เป็นต้น

I: Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น ข้อมูลของธนาคารด้านการเงิน ข้อมูลบัญชีธนาคาร ข้อมูลที่อยู่บนระบบคอมพิวเตอร์ เป็นต้น

A: Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล

2. รูปแบบภัยคุมคามของ Cybersecurity

สรุป 11 ภัยคุกคามที่เกิดขึ้นในปี 2020 จากตัวอย่างขององค์กรของฝั่งยุโรปที่ดูแลเรื่องภัยคุกคามทางไซเบอร์ (ENISA) ได้ดังนี้

1. Malware คือ ซอฟต์แวร์หรือ code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์นั้น และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ ได้ โดยพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ครอบคลุมถึงไวรัส (Virus) เวิร์ม (Worms) โทรจัน (Trojans) ด้วย

2. Web-based attack คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้วจะนำเหยื่อไปที่เป้าหมายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

3. Phishing คือ วิธีการโจมตีเหยื่อผ่านช่องทางต่าง ๆ เช่น e-mail, SMS, เว็บไซต์ หรือ ช่องทาง social โดยใช้วิธีหลอกหล่อเหยื่อด้วยวิธีต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น username, password หรือข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

4. Web application attack คือ วิธีการโจมตีเว็บไซต์เป้าหมาย โดยอาศัยช่องโหว่ต่าง ๆ เช่น code ของเว็บไซต์ Web server หรือ Database server วิธีการโจมตีที่นิยมใช้ ได้แก่ Cross-Site Scripting, SDL injection, Path Traversal เป็นต้น

5. Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล ข้อความ หรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น e-mail, SMS, เว็บไซต์ หรือช่องทาง social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญหรือก่อกวน

6. DDos (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ ระบบการให้บริการหรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์ ระบบการให้บริการ ระบบเครือข่ายไม่สามารถใช้งานหรือระบบล่มได้

7. Data Breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ ข้อมูลของแอปพลิเคชั่น หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการ แอปพลิเคชั่นหรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ

8. Insite threat คือ ภัยที่เกิดจากบุคลากรภายในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่งถือว่าเป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรงมาก โดยมีวิธีป้องกัน ได้แก่ นำหลักการ Zero Trust มาใช้ภายในองค์กร โดยการตรวจสอบผู้เข้าระบบทุกครั้ง และให้สิทธิ์ที่น้อยที่สุดหรือเท่าที่จำเป็นกับผู้ใช้งาน

9. Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดีที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา แต่จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิตหรือผู้ไม่ประสงค์ดี

10. Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware คือ ทำการล็อคไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์ เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง วิธีการป้องกัน ได้แก่ สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล และควรติดตั้ง Anti-Malware และมีการอัพเดทอย่างสม่ำเสมอ

11. Cryptocurrency คือ เหรียญดิจิตอล ซึ่งจะมีการประมวลผลตลอดเวลา ซึ่งในการประมวลผลจำเป็นที่จะต้องใช้ในส่วนของ CPU หรือ GPU หรือการ์ดจอเครื่องคอมพิวเตอร์ทำการประมวลผล และหลังจากประมวลผลเสร็จเรียบร้อยก็จะส่งกลับไปที่ส่วนกองกลางของเหรียญนั้น ๆ เพื่อที่จะได้รับค่าตอบแทนในการประมวลผล

3. ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

1. คอมพิวเตอร์ (Computer) สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ดังนี้ (1) ควรมีการแยก user ใช้งานกันของแต่ละบุคคล (2) ควร logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์ (3) ควรติดตั้ง Anti-Malware และมีการอัพเดทอย่างสม่ำเสมอ (4) มีการอัพเดท Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ (5) มีการอัพเดทเวอร์ชั่นของโปรแกรมบนเครื่องอย่างสม่ำเสมอ (6) ไม่ควรจด password หรือติด password ไว้ที่หน้าจอ และ (7) มีการใช้ password ที่ดีและไม่บอก password แก่ผู้อื่น

2. รหัสผ่าน (Password) โดยการใช้ password ที่ดี คือ (1) มีความซับซ้อน เช่น password ประกอบด้วย ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (2) มีความยาวของ password อย่างน้อย 8 ตัวอักษร (3) ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น password, 123456, วันเกิด, หมายเลขโทรศัพท์ เป็นต้น (4) มีการเปลี่ยน password อย่างสม่ำเสมอ (5) ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้ (6) ไม่ควรใช้ password ซ้ำกันในแต่ละระบบ และไม่บอก password แก่ผู้อื่น

3. E-mail สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ดังนี้ (1) ไม่เปิด e-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน (2) ไม่เปิดไฟล์แนบจาก e-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน (3) ไม่คลิกลิงค์ใน e-mail โดยไม่มีการตรวจเช็ค และ (4) เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการเช็คผ่านช่องทางอื่นๆ เพิ่มเติม

4. Website สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ดังนี้ (1) ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด (2) ไม่ควรทำการบันทึก password ต่าง ๆ บน Browser (3) เว็บไซต์สำหรับการทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน https เท่านั้น (4) ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla, Firefox เป็นต้น (5) ควรมีการอัพเดทเวอร์ชั่นของ Browser อย่างสม่ำเสมอ (6) ในกรณีที่เครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัว ควรใช้งาน Browser ในโหมด safe web browsing และ (7) ควรติดตั้ง Anti-Malware และอัพเดทอย่างสม่ำเสมอ

5. Messaging สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ดังนี้ (1) ไม่ควรบันทึก password ไว้ที่โปรแกรม (2) กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง และ (3) มีความตระหนักก่อนเปิดลิงค์หรือไฟล์ต่าง ๆ ที่ได้รับมา

6. Fake News หรือข่าวปลอม เป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก ทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้ วิธีการสังเกตข่าวปลอม ได้แก่ (1) มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ (2) ระบุที่มาของข่าวไม่ได้ (3) มักไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์ และ (4) สำนวนการเขียนออกแนวโฆษณา เป็นต้น

7. Conference สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ดังนี้ (1) ใช้สถานที่ที่เหมาะสมกับการ Conference (2) ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง (3) แชร์เอกสารต่าง ๆ อย่างระมัดระวัง (4) ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน และ (5) มีการอัพเดทเวอร์ชั่นของโปรแกรม Conference อย่างสม่ำเสมอ

8. Cloud storage สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ดังนี้ (1) แยก user ในการใช้งานของแต่ละบุคคล (2) ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น (3) ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์ที่ไม่มีความจำเป็น (4) ควรติดตั้ง Anti-Malware และอัพเดทอย่างสม่ำเสมอ และ (5) มีการตั้ง password และไม่ควรบอก password แก่ผู้อื่น

สิ่งที่เราควรทำในการสร้างความตระหนักรู้ความมั่นคงทางไซเบอร์ คือ ควรพยายามถ่วงน้ำหนักระหว่างเรื่องความปลอดภัยทางด้าน Cybersecurity กับความสะดวกสบายให้เท่ากัน กล่าวคือ เราควรตระหนักเสมอว่าความสะดวกสบายในการใช้งานน้อยลง ไม่บันทึก password ไว้ที่โปรแกรมเพื่อความสะดวกสบาย นั่นหมายความว่าความมั่นคงปลอดภัยทางไซเบอร์ การรอดพ้นจากการถูกโจมตีในรูปแบบต่าง ๆ มีเพิ่มมากขึ้น

ประโยชน์ที่ได้รับต่อตนเอง

ได้เรียนรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในการทำงานและได้รับความรู้เกี่ยวกับการป้องกันภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ และสามารถนำความรู้ที่ได้มาประยุกต์ใช้ในการทำงานและในชีวิตประจำวันได้

ประโยชน์ที่ได้รับต่อหน่วยงาน

ทำให้บุคลากรของหน่วยงานมีความเข้าใจและตระหนักถึงความมั่นคงปลอดภัยทางไซเบอร์ ในการนำเครื่องมือทางด้านเทคโนโลยีและวิธีการป้องกันต่างๆ มาประยุกต์ใช้ในการเตรียมพร้อมรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย ของหน่วยงานได้มากยิ่งขึ้น