สรุปความรู้ที่ได้จากการเข้าอบรม

"การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness"

ผ่านการพัฒนาทางไกลด้วยระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ (E-Learning)

รอบที่ ๑/๒๕๖๖ : ตุลาคม ๒๕๖๕ - มีนาคม ๒๕๖๖

โดย ว่าที่ร้อยตรีหญิง วชิรฎาพร ครื้นอุระ ตำแหน่ง เจ้าพนักงานการเกษตรปฏิบัติงาน

สังกัด กลุ่มวิชาการเพื่อการพัฒนาที่ดิน สำนักงานพัฒนาที่ดินเขต ๖

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness

Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยีวิธีการปฏิบัติที่ผ่านกระบวนการออกแบบไว้เพื่อป้องกันและรับมือการโจมตีที่อาจเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากที่ถูกโจมตีจากบุคคลที่สามโดยไม่ได้รับอนุญาต

ปัจจุบันหน่วยงานภาครัฐ และเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมาย และรูปแบบในการโจมตีมีหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้น

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

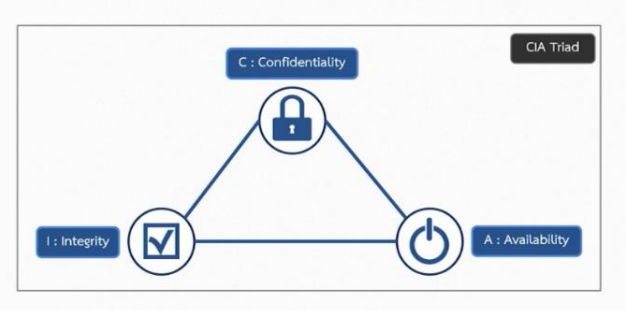
๑. พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ ๒๕๖๒

๒. พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ ๒๕๖๐

๓. พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

๔. มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ ระบบบริหารจัดการความปลอดภัยของข้อมูล

หลักกการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์



Confidentiality (C) หรือ การรักษาความลับของข้อมูล

คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ เช่น

- ข้อมูลเงินเดือนของพนักงานในบริษัท จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น
- เบอร์โทรของพนักงานบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

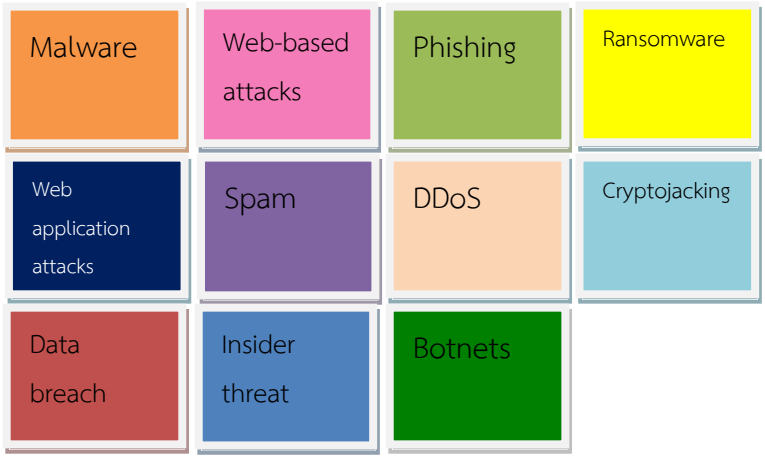
Intergrity (I) หรือ การรักษาความถูกต้องของข้อมูล

คือ การระบุสิทธิการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง
เช่น - ข้อมูลธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร - ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

Availability (A) หรือ ความพร้อมใช้งานของข้อมูล

คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น
- ข้อมูลธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

รูปแบบภัยคุกคามของ Cybersecurity



รูปแบบภัยคุกคามของ Cybersecurity

๑. **Malware** คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอ่านแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึง Server ต่างๆ ได้โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา เช่น ไวรัส (Virus) เวิร์ม (Worms) โทรจัน (Trojans)

๒. **Wed-based attacks** คือ วิธีการโจมตีเหยื่อผ่านช่องทางเว็บไซต์หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่โค้ดเมื่อเหยื่อเข้ามาเว็บไซต์ดังกล่าว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

๓. **Phishing** คือวิธีการโจมตีเหยื่อหาช่องทางต่างๆ เช่น E-mail, SMS เว็บไซต์หรือช่องทาง Social โดยใช้หลอกล่อเหยื่อด้วยวิธีการต่างๆที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น username, Password หรือข้อมูลสำคัญอื่นๆเพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

๔. **Web application attacks** คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น

- Code ของเว็บไซต์ เช่น cms
-Web Server หรือ database Server

วิธีการโจมตีที่นิยมใช้

-Cross-Site pcripting - SQL injection

๕. **Spam** คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูลข้อความหรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น E-mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยเป็นการส่งจำนวนมากหรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญหรือก่อกวน

๖. **DDos** คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์,ระบบการให้บริการหรือระบบเครือข่ายโดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกันจุดประสงค์ที่ทำเพื่อให้เว็บไซต์ ,ระบบการให้บริการหรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

๗. **Data breach** คือเกิดการรั่วไหลของข้อมูล ที่อาจเกิดจากช่องโหว่หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูลของ Application หรือระบบที่ทำให้บริการต่างๆโดยที่เจ้าของข้อมูลหรือผู้ให้บริการ Application หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขายหรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

ผลกระทบ

- ข้อมูลสำคัญส่วนตัวหรือขององค์กรโดนนำไปเผยแพร่
- ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
- สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

๘. **Insider Threat** คือ ภัยที่เกิดจากภายในบุคลากรในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจหากช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือสมาร์ทโฟน เป็นต้นซึ่งเป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

วิธีการป้องกันนำหลักการ Zero Trust มาใช้ภายในองค์กร

๙. **Botnet หรือ Robot Network** คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการอย่างที่ถูกโปรแกรมไว้ ส่วนมากจะแฝงตัวบเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets ที่ไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๑๐. **Ransomware คือ Walware** ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าถ่ายของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน

- สำรองข้อมูลเป็นประจำโดยทำการแยกที่เก็บไฟล์สำรองข้อมูล
- ควรติดตั้ง Anti-Malware และมีการอัพเดทอย่างสม่ำเสมอ
- ก่อนเปิดไฟล์ต่างๆ ที่ได้รับมาควรมีการตระหนักก่อนที่จะทำการเปิด

๑๑. **Cryptojacking** คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้ในการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อตามประเมินผลเพื่อสร้างรายได้กลับไปที่ Hacker

ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

คอมพิวเตอร์

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ควรมีการแยก User ใช้งานการของแต่ละบุคคล

๒. ควรออกจากระบบเมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

๓. ควรติดตั้ง Anti Malware และมีการอัพเดทอย่างสม่ำเสมอ

๔. มีการอัพเดทระบบปฏิบัติการ OS อย่างสม่ำเสมอ

๕. มีการอัพเดทเวอร์ชั่นของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๖. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ

๗. มีการใช้ Password ที่ดี และไม่บอก Password แก่ผู้อื่น

Password

๑. การใช้ Password ที่ดีคือหนึ่งมีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ

๒. มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร

๓. ความหลีกเลี่ยงการใช้ Common Password หรือ Default Password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น Password ๑,๒,๓,๔,๕,๖ วันเกิด และหมายเลขโทรศัพท์

๔. มีการเปลี่ยน password อย่างสม่ำเสมอ

อีเมล์

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เปิด Gmail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

๒. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

๓. ไม่คลิกลิงค์ใน E-mail โดยไม่มีการตรวจเช็ค

๔. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆควรมีการเช็คผ่านเข้าทางอื่นๆเพิ่มเติม

เว็บไซต์

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ได้เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่ชัดเจนเช่นการใช้งานช่องทาง Social ต่างๆ

๒. ไม่ควรทำการบันทึก Password ต่างๆบนบราวเซอร์

๓. เว็บไซต์สำหรับทำธุรการที่สำคัญหรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน https

๔. ควรมีการอัพเดทเวอร์ชั่นของเราสม่ำเสมอ

๕. ในกรณีเครื่องคอมพิวเตอร์ที่ไม่ใช่เรื่องส่วนตัวควรใช้งาน Browser ในโหมดเซฟเว็บ Save Web browsing

๖. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งานเช่น Google Chrome , mozilla Firefox เป็นต้น

Message

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรให้ระบบจำ Password ไว้ที่โปรแกรม

๒. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัวไม่ควรบันทึกไฟล์ต่างๆไว้บนเครื่อง

๓. มีความตระหนักก่อนเปิดลิงก์หรือฝ่ายต่างๆที่ได้รับมา

๔. มีการ update Version ของโปรแกรมอย่างสม่ำเสมอ

๕. ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล

Fake News

ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่ดูมีความน่าเชื่อถือ ทำให้ผู้ที่ได้ข่าวสารหลงเชื่อสามารถสร้างกระแสปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านช่องทางออนไลน์ เช่น LINE Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น

วิธีการสังเกตข่าวปลอม

๑. มีการพาดหัวข่าวหรือข้อความที่เกินจริงเพื่อสร้างความน่าสนใจ

๒. ระบุที่มาของข่าวไม่ได้

๓. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์

๔. สำนวนการเขียนออกมาแนวการโฆษณา

Conference

สิ่งที่ต้องควรปฏิบัติเพื่อความปลอดภัย

๑. ใช้สถานที่เหมาะสมกับการ Conference

๒. ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง

๓. แชร์ข้อมูลต่างๆ อย่างระมัดระวัง

๔. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน

๕. มีการ update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

Cloud storage

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. แยก User ในการใช้งานของแต่ละบุคคล

๒. ควรกำหนดผู้เข้าสู่ไฟล์ได้เท่าที่จำเป็นเท่านั้น

๓. ปิดการเข้าถึงไฟล์หรือปิดการแชร์ไฟล์ เมื่อไม่มีความจำเป็น

๔. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

๕. มีการ update Version ในโปรแกรมอย่างสม่ำเสมอ

๖. มีการตั้ง Password ที่ดีและมันบอก Password แก่ผู้อื่น

สรุป

เหตุการณ์โดยเจตนาที่มีการละเมิดและเข้าถึงระบบคอมพิวเตอร์ เครือข่าย หรือสิ่งอำนวยความสะดวกที่เชื่อมต่อโดยไม่ได้รับอนุญาตนั้นเรียกว่าการโจมตีทางไซเบอร์ อาชญากรไซเบอร์ มีวิธีการที่พลิกแพลงมากขึ้นเรื่อย ๆ ในการพยายามเข้ามาขโมยข้อมูลและดึงข้อมูล ซึ่งจะทำให้พวกเขาโจมตีข้อมูลต่าง ๆ เช่น บัญชีเงินฝาก ข้อมูลประจำตัวของคุณ และในอนาคตอันใกล้นี้ ยังรวมถึงข้อมูลด้านสุขภาพ หรือที่เกี่ยวข้องกับชีวิตจึงต้องรักษาความปลอดภัยทรัพย์สินดิจิทัลและปกป้องระบบของตน ให้ระวัง! ตื่นตัวอยู่ตลอดเวลา! สิ่งนั้นเป็นสิ่งที่น่าสงสัย! ให้ปฏิบัติตามกฎการรักษาความปลอดภัยเครือข่ายที่ยอมรับโดยทั่วไป