แบบฟอร์ม Knowledge Capture

สรุปโดย นางสาวฑิฆัมพร เส่งเจริญ พนักงาน (ระดับ 4) งานควบคุมระบบงาน ส่วนตรวจสอบสารสนเทศ ฝ่ายตรวจสอบข้อมูลบัญชีการเงินและสารสนเทศ สำนักตรวจสอบภายใน

1. บริบท หรือความเป็นมา

1. ตามบันทึกสั่งการ (นายชาญณรงค์ อินทนนท์) รองผู้อำนวยการปฏิบัติการแทนผู้อำนวยการองค์การอุตสาหกรรมป่าไม้ ลงวันที่ 8 กันยายน 2565 ท้ายบันทึก ออป.ตะวันออกเฉียงเหนือ ที่ ทส 1411.1/10105 ลงวันที่ 5 กันยายน 2565 เรื่องแจ้งเหตุเครื่องคอมพิวเตอร์ในกลุ่มเครือข่าย ออป.ตะวันออกเฉียงเหนือ และ ออป.เขตขอนแก่น พบไวรัสเรียกค่าไถ่ (Ransomware) ทราบ และเห็นความแจ้งทุกสำนักทราบ นั้น

2. สำนักตรวจสอบภายใน ได้ดำเนินการสอบทานการปฏิบัติงานของ ออป. ตะวันออกเฉียงเหนือ ตามบันทึก ส.ตส. ที่ ทส 1402.2/10075 ลงวันที่ 27 ตุลาคม 2565 เรื่องรายงานผลการตรวจสอบตามแผนการตรวจสอบประจำปี 2565 (องค์การอุตสาหกรรมป่าไม้ภาคตะวันออกฉียงเหนือ) ด้านสารสนเทศ (การควบคุมทั่วไป, การควบคุมระบบงาน) ระบบเครือข่ายคอมพิวเตอร์ เห็นควรให้ ออป.ตะวันออกเฉียงเหนือ ประสาน ส.วป. ในการขอใช้ระบบสำรองข้อมูล (Backup) รวมทั้งมีการสำรองข้อมูลอย่างต่อเนื่อง และสร้างการรับรู้โดยมีการถ่ายทอดถึงผู้ปฏิบัติงานทุกระบบปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัยเว็บไซต์ ในการเข้าใช้งานระบบเครือข่ายอินเตอร์เน็ตอย่างปลอดภัย

2. วิธีการ / ขั้นตอน หรือกระบวนการที่ได้เรียนรู้

สำนักตรวจสอบภายใน ขอเรียนว่า เพื่อเป็นการตระหนักถึงเหตุการณ์ที่เกิดขึ้น และเป็นการสร้างการรับรู้ให้ผู้ปฏิบัติงานในองค์กร ในฐานะผู้ตรวจสอบภายในมีหน้าที่บริการด้านการให้คำปรึกษา และเป็นการต่อยอดองค์ความรู้ โดยมีการดำเนินการดังนี้

1. นางสาวฑิฆัมพร เส่งเจริญ พนักงานควบคุมระบบงาน ส่วนตรวจสอบสารสนเทศ ฝ่ายตรวจสอบข้อมูลบัญชีการเงินและสารสนเทศ สำนักตรวจสอบภายใน เข้ารับการอบรมหลักสูตรออนไลน์ จากกรมพัฒนาฝีมือแรงงาน กระทรวงแรงงาน หลักสูตร ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Basic Cybersecurity) เรียบร้อยแล้ว จึงขอส่งใบประกาศนียบัตร และรายงานผลเข้ารับการฝึกอบรมตามแบบรายงานสรุปผล

2. จัดทำองค์ความรู้ในรูปแบบวีดีโอผ่านช่องทาง Youtube และจัดทำแบบการทดสอบออนไลน์ด้วยระบบอิเล็กทรอนิกส์ Google Forms เรื่อง “ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Basic Cybersecurity)” โดยเมื่อทำแบบทดสอบผ่านเกณฑ์ ร้อยละ 80 จะได้รับเกียรติบัตรอิเล็กทรอนิกส์ผ่านทางอีเมล์ที่ลงทะเบียนไว้ (เกียรติบัตรอิเล็กทรอนิกส์ออกในนามสำนักตรวจสอบภายใน)

3. เทคนิคหรือกลยุทธ์ที่สามารถนำไปสู่การปฏิบัติได้

- เพื่อให้ผู้ที่ศึกษามีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
- เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับภัยคุกคามประเภทต่างๆ และแนวทางป้องกันแก้ไข
- เพื่อให้ผู้เรียนสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

4. ประเด็นความรู้ที่สำคัญ

การป้องกันภัยคุกคามทางด้านไซเบอร์ (Cyber Security)

ภัยบนโลกไซเบอร์มีอยู่ 5 รูปแบบหลัก

1. CRITICAL INFRASTRUCTURE SECURITY

ในสังคมที่ใช้งานอยู่ในปัจจุบัน เช่นระบบโครงข่ายไฟฟ้า ระบบประปา ระบบจราจร ระบบข้อมูลคนไข้ในโรงพยาบาล เป็นต้น ส่วนมากจะเห็นข่าวในเรื่องของการโจรกรรมข้อมูลที่เป็นข้อมูลคนไข้โรงพยาบาล

2. APPLICATION SECURITY

โปรแกรมที่ใช้งานในระบบคอมพิวเตอร์ทั้งในฝั่งของซอฟต์แวร์และฮาร์ดแวร์ซึ่งถูกแบ่งออกเป็น 2 ส่วน

1) โปรแกรมที่เราใช้งานเพื่อประโยชน์เช่น microsoft word excel powerpoint หรือMicrosoft Edge ในเรื่องของเว็บบราวเซอร์ เป็นต้น

2) โปรแกรมที่เกี่ยวกับ Security เช่น โปรแกรม Antivirus ที่ใช้ในการตรวจสอบไวรัสในเครื่อง โปรแกรมที่เป็นในเรื่องของ Windows Firewall เป็นต้น ในเรื่องการปลอมแปลงข้อมูลว่าใครสามารถเข้าถึงเครื่องได้บ้างหรือโปรแกรมที่มีการเข้ารหัสข้อมูลซึ่งเป็นการเข้ารหัสข้อมูลในรูปแบบของเจ้าของเครื่องเอง ไม่ใช่เครื่องเราถูกสิ่งแปลกปลอมเข้ารหัสหรือที่เรียกว่า Ransomware

3. NETWORK SECURITY

ในปัจจุบันเราใช้งานผ่านระบบเครือข่าย ไม่ว่าจะเป็นในฝั่งของเครือข่ายโทรศัพท์มือถือเครือข่ายอินเทอร์เน็ตที่เราใช้ผ่านทางโทรศัพท์มือถือผ่านทั้งเครื่องแท็บเล็ท ผ่านทางเครื่องคอมพิวเตอร์ เป็นต้น ซึ่งการเข้าถึงข้อมูลดังกล่าว มีผู้ใช้งานในรูปแบบผู้ใช้งานโดยทั่วไปและผู้ใช้งานในที่มุ่งเน้นในเรื่องของการโจรกรรมข้อมูล เป็นต้นจึงจำเป็นต้องปกป้องในส่วนของเน็ตเวิร์คไม่ให้มีการแปลกปลอมเข้ามาสู่ระบบได้ กระบวนการการป้องกัน คือการใช้ FIREWALL เข้ามาจัดการแยกระหว่างเน็ตเวิร์กตนเอง กับเน็ตเวิร์กอื่นๆ เพื่อกรองการเข้าถึงข้อมูลนั่นเอง

4. CLOUD SECURITY & CLOUD COMPUTING

ปัจจุบันหลายๆองค์กรเริ่มมีการใช้งานในส่วนของเขา ระบบคลาวด์ ไม่ว่าจะเป็นในฝั่งของ Microsoft 365 ในฝั่งของ google apps เป็นต้น ซึ่งสามารถจัดเก็บข้อมูลทั้งหมดวางไว้บนระบบอินเตอร์เน็ต การเข้าถึงข้อมูลก็ต้องเป็นกระบวนการในเรื่องของการควบคุมในฝั่งของ Cloud resources โดยมีเครื่องมือต่างๆในเรื่องของ security ให้เราได้ใช้งานในเรื่องของความปลอดภัยก็ขึ้นอยู่กับผู้ให้บริการ ว่าผู้ให้บริการนั้นมีเครื่องมืออะไรที่เราได้ใช้งานบ้างเช่นกัน

5. INTERNET OF THINGS (IOT) SECURITY

ในปัจจุบันอุปกรณ์ต่างๆ เช่น ทีวี เครื่องปริ้น กล้องวงจรปิด สามารถเข้าถึงข้อมูลต่างๆ ผ่านอินเตอร์เน็ตได้ หมายความว่าเมื่อเราเข้าถึงอินเทอร์เน็ตได้ก็จะมีบุคคลที่อาจจะไม่ใช่เราพยายามเข้าถึงอุปกรณ์นั้นๆ ด้วยฉะนั้นเราต้องมีวิธีป้องกันอย่างไรสำหรับการที่ไม่ให้บุคคลนั้นๆเข้ามาใช้งานอุปกรณ์ของเรานั่นเอง

การป้องกันมัลแวร์ (MALWARE)

มัลแวร์ คือซอฟต์แวร์หรือโปรแกรมที่ถูกนักพัฒนาพัฒนาขึ้นมาเพื่อมุ่งเน้นในเรื่องของการสร้างผลกระทบให้กับระบบคอมพิวเตอร์ไม่ว่าจะเป็นการมุ่งเน้นในเรื่องของการทำลายข้อมูล การทำลายระบบหรือทำลายโปรแกรม ส่วนมากจะเรียกว่า “ซอฟต์แวร์ไม่พึงประสงค์”

ชนิดของมัลแวร์

ไวรัส (Virus) มีลักษณะการแพร่เชื้อไปติดไฟล์อื่นๆในคอมพิวเตอร์โดยการแนบตัวเองเข้าไป ไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆได้คือต้องอาศัยไฟล์และ Removable Drive สิ่งที่ทำคือสร้างความเสียหายให้กับไฟล์งานและไฟล์โปรแกรมต่างๆ

มัลแวร์เรียกค่าไถ่ (RANSOMWARE) หรือไวรัสเรียกค่าไถ่ ถือเป็นมัลแวร์ประเภทหนึ่ง หลังจากเครื่องเป้าหมายติดมัลแวร์ คอมพิวเตอร์จะถูกเข้ารหัส หรือบล็อกการเข้าถึงข้อมูลบนดิสก์ แล้วแจ้งหรือยื่นข้อเสนอให้เหยื่อ สำหรับโอกาสความเป็นไปได้ของการกู้คืน โดยจะให้เหยื่อทำการโอนเงินไปยังบัญชีที่ระบุของผู้ไม่ประสงค์ดี

สปายแวร์ (SPYWARE) จะดักจับข้อมูลเกี่ยวกับกิจกรรมของคุณ โดยดึงข้อมูลจากไดรฟ์ของคุณ ขโมยไฟล์ข้อมูล การเข้าสู่ระบบ ข้อมูลบัญชีธนาคาร บัตรเครดิตของคุณ และยังตรวจสอบกิจกรรมของคุณทั้งหมด

ฟิชชิ่ง (PHISHING) อาชญากรไซเบอร์ที่ใช้การโจมตีโดยมีเป้าหมายเป็นข้อมูลส่วนบุคคลของคุณเอง เช่น หมายเลขบัตรเครดิต เลขบัตรประจำตัวประชาชน รหัสผ่าน เพื่อนำไปสู่การเข้าสู่ระบบบัญชีออนไลน์ของคุณ เป็นการโจมตีที่นิยมและพบบ่อยที่สุด

พฤติกรรมการใช้งานที่เสี่ยงต่อความปลอดภัย

- ติดตั้งโปรแกรมโดยไม่อ่านรายละเอียด
- แอบเล่นอินเตอร์เน็ตไร้สายฟรี
- ติดตั้งโปรแกรมแอนตี้ไวรัสปลอม
- คลิก link หรือเปิดไฟล์แนบที่มากับอีเมลโดยไม่ตรวจสอบ

วิธีการสังเกตุอาการผิดปกติจากมัลแวร์

สังเกตความผิดปกติของเครื่องคอมพิวเตอร์ของเรา เช่น

- เปิดเครื่องทิ้งไว้ไม่ได้ใช้งานแต่ตัวชี้เม้าส์ (mouse pointers) เคลื่อนที่เองได้
- รู้สึกว่าเครื่องคอมพิวเตอร์ช้าผิดปกติ
- แฟ้มข้อมูลใช้งานไม่ได้

ซอฟแวร์ที่ป้องกันมัลแวร์

- ติดตั้งโปรแกรมแอนตี้ไวรัส (แอนตี้มัลแวร์)
- การอัพเดทซอฟแวร์แพทช์ (Update Virus Definitions)

การป้องกันความเสียหายของข้อมูลจากมัลแวร์

- สำเนาข้อมูลไว้ที่ USB Drive
- สำเนาข้อมูลไว้ที่ Cloud Storage เช่น One Drive

5. บทสรุป

ปัจจุบันเราใช้อุปกรณ์ต่างๆ เช่น เครื่องคอมพิวเตอร์ โทรศัพท์มือถือ ทีวี ตู้เย็นหรืออีกหลายๆอย่าง ที่เชื่อมต่ออินเตอร์เน็ตได้ อุปกรณ์เหล่านั้นล้วนแต่มีข้อมูล ซึ่งข้อมูลอาจจะเป็นข้อมูลที่ละเอียดอ่อนมากหรือละเอียดอ่อนน้อยก็แล้วแต่ว่าจะเป็นเป้าหมายของกลุ่มบุคคลที่เรียกว่าแฮกเกอร์ ที่จะมุ่งเน้นเข้ามาโจรกรรมข้อมูลเราจำเป็นต้องป้องกันการถูกโจรกรรมด้วยวิธีการเบื้องต้น เพื่อป้องกันในส่วนของสิ่งแปลกปลอมที่จะเข้ามาสู่เครื่องในการปฏิบัติงาน