

สรุปบทเรียน หลักสูตร การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (Cybersecurity)

ระบบเรียนออนไลน์ e - Learning ของสถาบัน TDGA

ผู้รับการฝึกอบรม : นางสาวนันท์วรรณ หมั่นมัน

ตำแหน่ง : เจ้าพนักงานธุรการปฏิบัติงาน

สังกัด : กลุ่มสารบรรณ สำนักงานเลขาธิการกรม

ความรู้พื้นฐานของ Cybersecurity

Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น **ความลับสูงสุด** ผู้ที่เข้าถึงได้ คือ **ผู้จัดการส่วน**

ทรัพยากรบุคคลเท่านั้น

- เบอร์โทรของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่เข้าถึงได้ คือ พนักงานบริษัททุกคน

รูปแบบภัยคุกคามของ Cybersecurity

Malware คือ ซอฟต์แวร์ หรือ code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถถึงทรัพยากรของระบบคอมพิวเตอร์ด้วย และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ ต่างๆ โดยมีพฤติกรรมแตกต่างกันตามผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง

- ไวรัส (Virus)
- เวิร์ม (Worm)
- โทรจัน (Trojans)

Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านทางเว็บไซต์ หรือ Hack เว็บไซต์ ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

Phishing คือ วิธีการโจมตีเหยื่อผ่านทางต่างๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและใช้ข้อมูลส่วนตัว เช่น Username, password หรือ ข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตี เพื่อขโมยข้อมูลของเว็บไซต์ ข้อมูล ของแอปพลิเคชัน หรือให้บริการระบบที่ให้บริการไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

- ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่
- ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
- สร้างผลกระทบต่อชื่อเสียงและความเชื่อถือขององค์กร

Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

วิธีป้องกัน - นำหลักการ Zero Trust มาใช้งานภายในองค์กร

Botnets Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัว อยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรองรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจำไม่ทราบว่ามีกรติดตั้ง Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

Ransomware คือ Malware ประเภทหนึ่งที่ถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อกไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่มีอยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งวัตถุประสงค์ของ Ransomware ทำการล็อกไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อกไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีป้องกัน - สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล

- ควรติดตั้ง Anti - Malware และมีการ Update อย่างสม่ำเสมอ

- ก่อนเปิดไฟล์ต่าง ๆ ที่ได้รับมา ควรมีความตระหนักก่อนที่จะทำการเปิด

Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรม ที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อ ประมวลผลเพื่อสร้างรายได้กลับไป Hacker

วิธีป้องกัน - สร้างความตระหนัก

- ติดตั้งซอฟต์แวร์ป้องกัน

- อัปเดตระบบป้องกันเครือข่าย

Computer สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

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 ที่ดี และ **ไม่ควรบอก Password แก่ผู้อื่น**

การใช้ Password ที่ดี คือ

๑. มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ \$ #)

๒. มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร

๓. ควรหลีกเลี่ยงการใช้ Common Password หรือ Default Password หรือ สิ่งที่สามารถเดาได้ง่าย

เช่น Password,๑๒๓๔๕๖,วันเกิด,หมายเลขโทรศัพท์

๔. มีการเปลี่ยน Password อย่างสม่ำเสมอ

๕. ใช้ Multi Authentication ในกรณีที่สามารถใช้งานได้

๖. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ

๗. **ไม่ควรบอก Password แก่ผู้อื่น**

ประโยชน์ที่ได้รับต่อตนเอง

ได้รับรู้ถึงสิ่งควรปฏิบัติต่อ Computer ที่ถูกต้อง และทำเป็นประจำ ตามข้างต้นที่กล่าวมา เพื่อความปลอดภัย Computer ทั้งของตนเอง และ Computer ของทางราชการ เพื่อป้องกันภัยคุกคามทางดิจิทัล