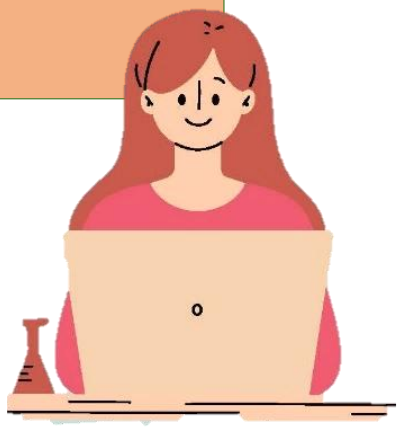
สรุปบทเรียน

หลักสูตร การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

(Cyber Security Awareness)



ผู้รับการฝึกอบรม : นางสาวอุบลวรรณ บำเรอวงศ์

ตำแหน่ง : นักจัดการงานทั่วไปชำนาญการ

สังกัด : กลุ่มสารบรรณ สำนักงานเลขานุการกรม

หน่วยงานที่จัดอบรม : สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

วัตถุประสงค์

เรียนรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงานและมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่าง ๆ และสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน

หัวข้อในบทเรียน

๑. ความรู้พื้นฐานของ Cybersecurity

๒. รูปแบบภัยคุกคามของ Cybersecurity

๓. ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

ผู้สอน

คุณพลากร ลาภอลงกรณ์

สรุปบทเรียน

Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยีวิธีการปฏิบัติที่ผ่านกระบวนการออกแบบไว้เพื่อป้องกันและรับมือการโจมตีที่อาจเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากที่ถูกโจมตีจากบุคคลที่ สามโดยไม่ได้รับอนุญาต ปัจจุบันหน่วยงานภาครัฐ และเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทาง ไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมาย และรูปแบบในการโจมตีมีหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้น

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

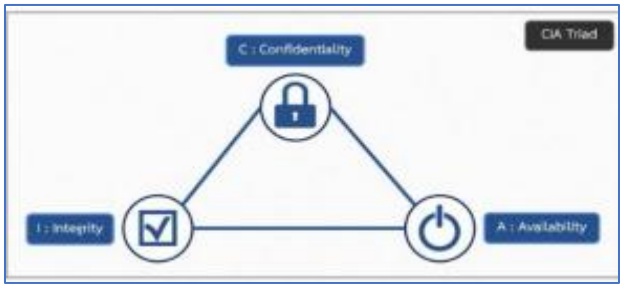
๑. พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ ๒๕๖๒

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

๓. พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

๔. มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ ระบบบริหารจัดการความปลอดภัยของข้อมูล

หลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์



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

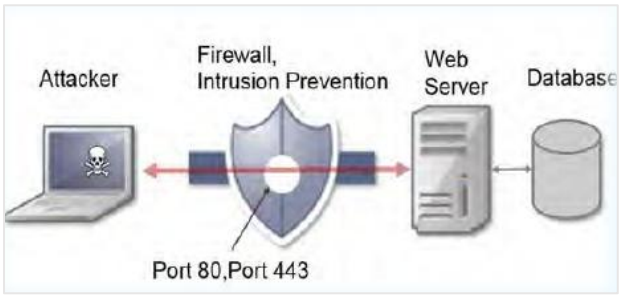
๑. Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึง ทรัพยากรของระบบคอมพิวเตอร์ และอ่านแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึง Server ต่างๆ ได้โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา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

๒. Wed-based attacks คือ วิธีการโจมตีเหยื่อผ่านช่องทางเว็บไซต์หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่โค้ดเมื่อเหยื่อเข้ามาเว็บไซต์ดังกล่าว จะนำเหยื่อไปที่เป้าหมายปลายทางที่ เป็นเว็บที่ทำการวาง 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

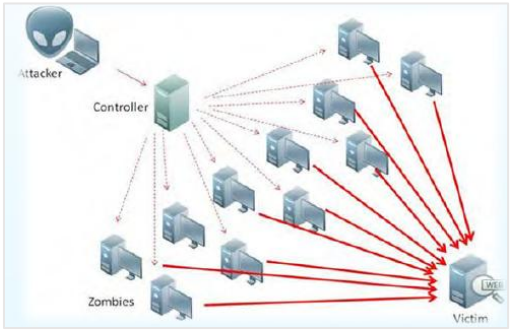


วิธีการโจมตีที่นิยมใช้

- Cross-Site pcripting
- SQL injection
- Path Traversal

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

๖. DDos (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์,ระบบการให้บริการหรือระบบเครือข่ายโดยใช้เครื่อง โจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้ เว็บไซต์,ระบบการให้บริการหรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม



๗. Data breach คือเกิดการรั่วไหลของข้อมูล ที่อาจเกิดจากช่องโหว่หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูลของ Application หรือระบบที่ทำให้บริการต่างๆโดยที่เจ้าของข้อมูลหรือผู้ให้บริการ Application หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขายหรือเพื่อเรียกค่าไถ่ของ ชุดข้อมูลนั้นๆ ผลกระทบ - ข้อมูลสำคัญส่วนตัวหรือขององค์กรโดนนำไปเผยแพร่ - ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล - สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

๘. Insider Threat คือ ภัยที่เกิดจากภายในบุคลากรในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจหากช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือสมาร์ทโฟน เป็นต้นซึ่งเป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง วิธีการป้องกันนำหลักการ Zero Trust มาใช้ภายในองค์กร

๙. Botnet หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตี เป้าหมายหรือดำเนินการอย่างที่ถูกโปรแกรมไว้ส่วนมากจะแฝงตัวบเครื่องของเหยื่อจะไม่ทราบว่ามี การติด Botnets ที่ไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

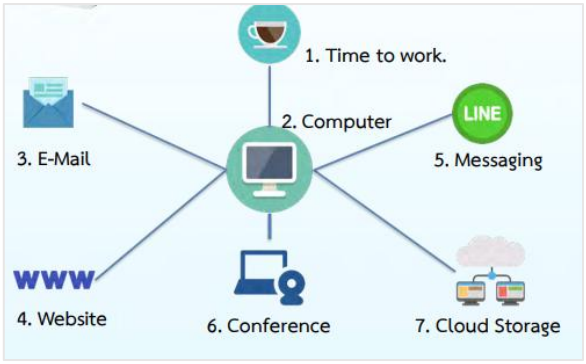
๑๐. Ransomware คือ Walware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์เพื่อที่จะเรียกค่าถ่ายของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน

- สำรองข้อมูลเป็นประจำโดยทำการแยกที่เก็บไฟล์สำรองข้อมูล
- ควรติดตั้ง Anti-Malware และมีการอัพเดทอย่างสม่ำเสมอ
- ก่อนเปิดไฟล์ต่างๆ ที่ได้รับมาควรมีการตระหนักก่อนที่จะทำการเปิด

๑๑. Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้ในการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่อง คอมพิวเตอร์ของเหยื่อตามประเมินผลเพื่อสร้างรายได้กลับไปที่ Hacker

ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน



๑) การใช้งานคอมพิวเตอร์

- ควรมีการแยก User ใช้งานกันของแต่ละบุคคล
- ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
- ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
- มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
- มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
- ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
- มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น

๒) การใช้ Password ที่ดี

- มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #)
- มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร
- ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password ๑๒๓๔๕๖ วันเกิด หมายเลขโทรศัพท์

- มีการเปลี่ยน Password อย่างสม่ำเสมอ
- ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้
- ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ
- ไม่ควรบอก Password แก่ผู้อื่น

๓) การใช้ E-mail

- ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
- ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
- ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค
- เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

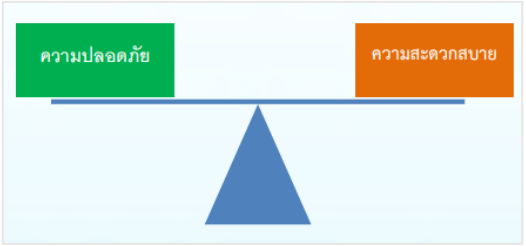
๔) การใช้ Website

- ไม่เข้าเว็บไซที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ
- ไม่ควรทำการบันทึก Password ต่างๆ บน Browser
- เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น

- ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น
- ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ
- ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing
- ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

สรุป

ในปัจจุบันเทคโนโลยีถูกพัฒนาให้ทันสมัยสะดวกสบายในการใช้งาน จนบางครั้งลืมคิดถึงเรื่องความปลอดภัยในชีวิตและทรัพย์สินของผู้บริโภค ดังนั้น หากจะกล่าวให้ถูกต้องควรมีความปลอดภัยที่มากขึ้นมาพร้อมกับความสดวกสบายที่ตามมา



ประโยชน์ที่ได้รับจากการอบรม

๑. ได้รับความรู้ ความเข้าใจและสามารถนำไปปรับใช้ในชีวิตประจำวันได้

๒. ได้รับความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่าง ๆ

****