รอบ2
ปีงบประมาณ
พ.ศ.2567

สรุปบทเรียนจากการพัฒนาความรู้

หลักสูตร การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (Cybersecurity Awareness)

จัดทำโดย นายฉัตรชัย เจริญสรรพสุข
นักวิชาการคอมพิวเตอร์ชำนาญการ

๑. นิยาม

ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่ ๓ โดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐและภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้น

ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

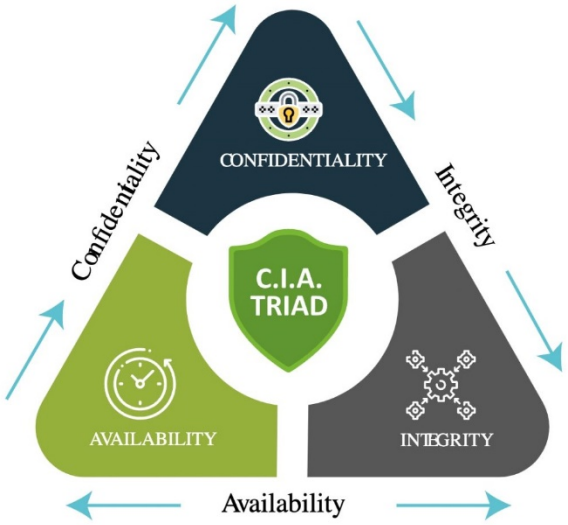
- พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐
- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
- มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

๒. พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ CIA Triad

๒.๑ Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิ์ในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละจุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น

๒.๒ Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิ์ของการแก้ไขข้อมูลและการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง ตัวอย่างเช่น ข้อมูลของธนาคารด้านการเงิน ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

๒.๓ Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น ข้อมูลของธนาคารด้านการเงิน ข้อมูลที่อยู่บนระบบคอมพิวเตอร์



ภาพที่ ๑ : CIA Triad

๓. รูปแบบภัยคุกคามของ Cyber Security

๓.๑ Malware คือ ซอฟต์แวร์หรือโค้ดประเภทหนึ่ง ที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์และอ่านแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์อื่นๆ ในเครือข่าย รวมถึง Server ต่างๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา โดยครอบคลุมถึง ไวรัส (Virus) เวิร์ม (Worms) โทรจัน (Trojans)

๓.๒ Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ โดยการใส่โค้ดที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้วจะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวางมัลแวร์ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติดมัลแวร์ โดยในปัจจุบันเว็บไซต์ส่วนใหญ่ที่โดนแฮกเพื่อแก้ไขโค้ดส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System) หรือเว็บไซต์ที่ใช้โค้ด open source เป็นหลัก

๓.๓ Phishing คือ วิธีการโจมตีเหยื่อผ่านช่องทางต่างๆ เช่น อีเมล SMS เว็บไซต์ หรือ ช่องทาง social media ต่างๆ โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการที่ทำให้หลงเชื่อและให้ข้อมูลส่วนบุคคล เช่น Username/Password หรือข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรมต่างๆ

๓.๔ Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น โค้ดของเว็บไซต์ Web Server หรือ database server เป็นต้น โดยจะมีวิธีการโจมตีที่นิยมใช้ หลากหลายรูปแบบ อาทิ Cross-Site Scripting, SQL injection, Path Traversal ซึ่งสามารถศึกษาวิธีป้องกันเพิ่มเติมได้จากมาตรฐาน OWASP top ten

๓.๕ Spam คือ วิธีการที่ผู้ส่งหรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล ข้อความ หรือโฆษณาต่างๆ ผ่านช่องทางไปยังผู้รับ เช่น อีเมล SMS เว็บไซต์ หรือช่องทาง social media โดยการส่งเป็นจำนวนมากหรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญหรือก่อกวน

๓.๖ DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ ระบบการให้บริการหรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางยิงจำนวนมากยิงมาที่เป้าหมายเดียวกัน ภายในเวลาเดียวกัน จุดประสงค์ที่ทำให้เว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

๓.๗ Data breach คือ การรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ ข้อมูลของ application หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการ application หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โดนตีต้องการนำข้อมูลไปขายหรือเรียกค่าไถ่ของชุดข้อมูลนั้นๆ โดยได้รับผลกระทบจากข้อมูลสำคัญส่วนตัวหรือขององค์กรที่โดนนำไปเผยแพร่ อาจมีการเรียกค่าไถ่ของชุดข้อมูล และสร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

๓.๘ Insider threat คือ ภัยที่เกิดจากภายใน บุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ภายในองค์กร หรือ สมาร์ทโฟน เป็นต้น ซึ่งเป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กรอาจจะมีการป้องกันในระดับต่ำทำให้เกิดการโจมตีประเภทนี้ได้ง่ายและผลลัพธ์ของภัยประเภทนี้มีความรุนแรงสูง

๓.๙ Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดีที่จะทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ โดยที่เจ้าของเครื่องไม่ทราบว่ามีการถูกติดตั้ง Botnets อยู่ เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ไม่ประสงค์ดี

๓.๑๐ Ransomware คือ มัลแวร์ประเภทหนึ่ง ที่ไม่ถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสข้อมูลไฟล์ทั้งหมดในเครื่องทำให้ข้อมูลที่อยู่บนเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์ เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

๓.๑๑ Cryptojacking คือ วิธีการที่พูดไม่ประสงค์ดีเข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไปที่ผู้ไม่ประสงค์ดี

๔. สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๔.๑ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยจากอุปกรณ์คอมพิวเตอร์

- ควรมีการแยก user ใช้งานกันของแต่ละบุคคล
- ควร logout เมื่อไม่อยู่หน้าจอเครื่องคอมพิวเตอร์
- ควรติดตั้ง Anti-Malware และมีการอัพเดทอย่างสม่ำเสมอ
- มีการอัพเดทแพทช์ระบบปฏิบัติการอย่างสม่ำเสมอ
- มีการอัพเดทเวอร์ชันของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
- ไม่ควรจด password หรือติด password ไว้ที่หน้าจอเครื่อง
- มีการใช้ password ที่ดีและไม่ควรบอก password แก่ผู้อื่น

๔.๒ การใช้ password ที่ดี

- มีความซับซ้อน เช่น ตัวอักษรใหญ่ ตัวอักษรเล็ก ตัวเลข และอักขระพิเศษ
- มีความยาวของ password อย่างน้อย ๘ ตัวอักษร
- ควรหลีกเลี่ยงการใช้ common password หรือ default password หรือสิ่งที่สามารถคาดเดาได้ง่าย
- มีการเปลี่ยน password อย่างสม่ำเสมอ

- ใช้ multifactor authentication ในกรณีที่สามารถใช้งานได้
- ไม่ควรใช้ password ซ้ำกันในแต่ละระบบ
- ไม่ควรบอก password แก่ผู้อื่น

๔.๓ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยจากอีเมล

- ไม่เปิดอีเมลที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
- ไม่เปิดไฟแนบจากอีเมลที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
- ไม่คลิกลิงค์ในอีเมลโดยไม่มีการตรวจเช็ค
- เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการตรวจเช็คผ่านช่องทางอื่นๆ เพิ่มเติม

๔.๔ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยจากเว็บไซต์

- ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่ชัดเจน
- ไม่ควรทำการบันทึก password ต่างๆ บน browser
- เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญ ต้องใช้งานผ่าน https เท่านั้น
- ใช้ browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน
- ควรมีการอัพเดทเวอร์ชันของ browser อย่างสม่ำเสมอ
- ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้ browser ในโหมด Safe Web Browsing
- ควรติดตั้ง Anti-Malware และอัพเดทอย่างสม่ำเสมอ

๔.๕ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยจาก Messaging

- ไม่ควรบันทึก password ไว้ที่โปรแกรม
- กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัวไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง
- มีความตระหนักก่อนเปิดลิงค์หรือไฟล์ต่างๆ ที่ได้รับมา
- มีการอัพเดทเวอร์ชันของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๔.๖ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยจาก Conference

- ใช้สถานที่เหมาะสมกับการ conference
- ในการประชุม conference ควรมีแต่ผู้ที่เกี่ยวข้องเท่านั้น
- การแชร์เอกสารต่างๆ ควรดำเนินการอย่างระมัดระวัง
- ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งานเท่านั้น
- มีการอัพเดทเวอร์ชันของโปรแกรม conference อย่างสม่ำเสมอ

๔.๗ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยจาก Cloud Storage

- แยก user ในการใช้งานของแต่ละบุคคล
- ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น
- ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น
- ควรติดตั้ง Anti-Malware และอัพเดทอย่างสม่ำเสมอ
- มีการอัพเดทเวอร์ชันของโปรแกรมอย่างสม่ำเสมอ
- มีการตั้ง password ที่ดีและไม่บอก password แก่ผู้อื่น

๔.๘ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยจาก Free Wifi

- ไม่ควรใช้งาน WiFi ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน
- หลีกเลี่ยงการใช้งาน WiFi ที่ไม่รู้ที่มาในการให้บริการ

๔.๙ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยจากโทรศัพท์เคลื่อนที่

- เปิดการใช้งาน PIN / password, Face Scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์
- ไม่ติดตั้ง application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา
- กำหนด application permission ให้เหมาะสม
- มีการอัพเดทแพทช์ระบบปฏิบัติการอย่างสม่ำเสมอ
- มีการอัพเดทเวอร์ชันของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๔.๑๐ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยจาก Internet Connection

- เปลี่ยน default password ของ router ที่มาจากค่าโรงงาน
- เปลี่ยน SSID และรหัสผ่านของ WiFi ที่กำหนดมาจากผู้ให้บริการ
- กำหนดผู้ที่สามารถเข้าใช้งานอินเตอร์เน็ตเท่าที่จำเป็นเท่านั้น

ภาพที่ ๒ : แสดงภัยคุกคามประเภทต่างๆ

แหล่งที่มา

หลักสูตร : การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness
บรรยายโดย : คุณพลากร ลาภอลงกรณ์ ผู้จัดการส่วนบริการลูกค้า ฝ่ายปฏิบัติการ
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
สถาบัน/หน่วยงาน/ระบบ : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล TDGA
รูปแบบหลักสูตร : e- Learning
ช่วงเวลาการฝึกอบรม : สิงหาคม 2567