หัวข้อการพัฒนา :

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

สรุปสาระสำคัญ

ปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากมีเป้าหมายและรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น ซึ่งจะสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อย ๆ โดยกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ ได้แก่ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560, พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และมาตรฐานด้านความปลอดภัย ISO 27001 ดังนั้น การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ จะเป็นการมุ่งเน้นการยกระดับความปลอดภัยให้หน่วยงานภาครัฐในยุคดิจิทัล โดยชี้ให้เห็นว่าระบบภาครัฐเป็นเป้าหมายสำคัญของภัยคุกคามที่หลากหลาย ความมั่นคงปลอดภัยนี้ไม่ได้ขึ้นอยู่กับระบบเทคโนโลยีเท่านั้น แต่อาจเกิดจากพฤติกรรมของบุคลากรในการทำงาน เช่น การใช้รหัสผ่าน หรือการเปิดอีเมล อาจกลายเป็นภัยเงียบจากภายใน บุคลากรจึงต้องเข้าใจหลักการรักษาข้อมูล เพื่อป้องกันการรั่วไหล การสร้างความตระหนักรู้จะช่วยเปลี่ยนบุคลากรให้เป็นเกราะป้องกัน เพื่อรักษาความน่าเชื่อถือขององค์กร

ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลอื่น โดยไม่ได้รับอนุญาต

หลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์หรือ CIA Triad เป็นแนวคิดหลัก 3 ประการในด้านความมั่นคงปลอดภัยทางไซเบอร์ ประกอบด้วย

1. การรักษาความลับของข้อมูล (Confidentiality) คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ เช่น ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท เบอร์โทรของพนักงานในบริษัท
2. การรักษาความถูกต้องของข้อมูล (Integrity) คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น ข้อมูลของธนาคารด้านการเงิน
3. ความพร้อมใช้งานของข้อมูล (Availability) คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น การมีระบบสำรองไฟฟ้า การมีแผนการกู้คืนระบบ

ในปัจจุบัน มีภัยคุกคามหลายประเภทและเป็นภัยคุกคาม ตัวอย่างเช่น

1. Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ ได้

2. Web-based attacks คือ วิธีการโจมตีโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ code ที่ทำให้เมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ติด Malware

3. Phishing คือ วิธีการโจมตีผ่านทางช่องทางต่าง ๆ เช่น E-Mail หรือ ช่องทาง Social โดยใช้วิธีการหลอกล่อด้วยวิธีการต่าง ๆ ที่ทำให้หลงเชื่อและให้ข้อมูลส่วนตัว เพื่อนำข้อมูลของเหยื่อไปใช้ในการทำธุรกรรม

4. Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น วิธีการโจมตีแบบ Cross-Site Scripting, SQL Injection, Path Traversal

5. Spam คือ วิธีการที่ผู้ไม่ประสงค์ดีทำการส่งข้อมูลผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail, SMS, โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญ หรือก่อกวน

6. DDoS คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ระบบการให้บริการหรือ ระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกันจุดประสงค์ที่ทำเพื่อให้เว็บไซต์ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

7. Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ

8. Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย

9. Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต

10. Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่าน ที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

11. Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์โดยวิธีการต่าง ๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ประมวณผลเพื่อสร้างรายได้กลับไปที่ Hacker

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยทางไซเบอร์ ดำเนินการได้ดังนี้

1. สร้างรหัสผ่านที่ซับซ้อน ควรสร้างรหัสที่มีความยาวอย่างน้อย 8 ตัวอักษร ประกอบด้วยอักษรตัวใหญ่ ตัวเล็ก ตัวเลข และสัญลักษณ์.

2. ห้ามใช้รหัสซ้ำ ควรแยก Password ของอีเมลทำงาน บัญชีธนาคาร และโซเชียลมีเดียส่วนตัวออกจากกันเด็ดขาด

3. เปิดใช้งานระบบยืนยันตัวตนสองชั้น (Multi-Factor Authentication) ในทุกแอปพลิเคชันที่รองรับเพื่อความปลอดภัยสูงสุด

4. สำรองข้อมูลสม่ำเสมอ ทำการ Backup ข้อมูลสำคัญและแยกเก็บไว้ต่างหาก เผื่อกรณีโดนภัยคุกคาม เช่น มัลแวร์เรียกค่าไถ่ (Ransomware)

การนำความรู้ไปใช้ประโยชน์

ได้รับความรู้และมีความเข้าใจ และตระหนักถึงความสำคัญของความมั่นคงปลอดภัยไซเบอร์ในการปกป้องระบบ อุปกรณ์ และข้อมูลจากการโจมตี และรู้เท่าทันรูปแบบภัยคุกคามสมัยใหม่ เพื่อนำไปใช้ในการเตรียมรับมือเพื่อความปลอดภัยในชีวิตประจำวันและองค์กร โดยมุ่งเน้นการปรับเปลี่ยนพฤติกรรมและการคิดก่อนคลิก เพื่อลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ในทุกช่องทาง พร้อมร่วมเป็นส่วนหนึ่งในการสร้างวัฒนธรรมความปลอดภัยทางดิจิทัล (Cybersecurity Culture) เพื่อปกป้องข้อมูลสำคัญขององค์กรและตนเองอย่างยั่งยืน