ตัวชี้วัด 4.21 : ระดับความสำเร็จของมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย
ขั้นตอนที่ 4 : สร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้กับเจ้าหน้าที่ของกรมอนามัย

การจัดประชุมส่งเสริมและสนับสนุนทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัลของกรมอนามัย (Digital Literacy) เรื่อง การสร้างความตระหนักด้านความมั่นคงทางไซเบอร์ (Cybersecurity Awareness) ในวันที่ 9 พฤษภาคม 2567 เวลา 09.30 - 16.30 น. ณ ห้องประชุมกองคลัง อาคาร 5 ชั้น 2 กรมอนามัย และระบบประชุมไกลออนไลน์ เพื่อให้เจ้าหน้าที่กรมอนามัยตระหนักถึงภัยคุกคามทางไซเบอร์ และเสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 มีรายละเอียด ดังนี้

1. สร้างความเข้าใจเกี่ยวกับอันตรายจากการโจมตีทางไซเบอร์ สามารถเกิดขึ้นได้ทุกเมื่อและมีผลกระทบที่หลากหลาย

1.1 แนวโน้มภัยคุกคามในปัจจุบัน ผู้โจมตีทางไซเบอร์หรือแฮกเกอร์ (Hacker) ใช้วิธีที่ซับซ้อนขึ้น เน้นสร้างความเสียหายทางเศรษฐกิจ หรือที่ส่งผลต่อความมั่นคงของชาติ โดยมีหลายรูปแบบด้วยกัน เช่น

- Sniffing คือ การดักจับข้อมูลที่มีการรับ-ส่งบนระบบเครือข่าย วิธีป้องกันคือ ไม่ควรใช้ระบบเครือข่ายฟรีทั่วไป (Free Wi-Fi) ในการทำกิจกรรมที่สำคัญ เช่น ธุรกรรมการเงิน เป็นต้น
- Spam คือ การส่งข้อความที่ผู้รับไม่ได้ร้องขอเป็นโฆษณาชวนเชื่อต่าง ๆ เช่น ทาง E-mail เป็นต้น
- Phishing คือ การหลอกลวงทางอินเทอร์เน็ต เช่น หลอกให้กดลิงก์ปลอม เพื่อให้กรอกข้อมูลที่สำคัญลงไป แล้วนำไปใช้ในทางที่ผิด
- Social Engineering คือ การใช้จิตวิทยาในการหลอกลวง เพื่อให้เปิดเผยข้อมูลที่เป็นความลับ
- Ransomware คือ มัลแวร์ที่สามารถบล็อกการเข้าถึงไฟล์บนเครื่องคอมพิวเตอร์/อุปกรณ์ของเหยื่อ เพื่อเรียกค่าไถ่ จึงจะได้รับการปลดบล็อกแล้วเข้าถึงไฟล์ได้อีกครั้ง
- Botnet คือ มัลแวร์ที่อาศัยอินเทอร์เน็ตที่เข้าไปเชื่อมกับคอมพิวเตอร์เหยื่อ เพื่อควบคุมการทำงาน
- Dos/DDos คือ การพยายามโจมตีระบบเครือข่ายคอมพิวเตอร์ เพื่อทำให้ไม่สามารถให้บริการนั้นได้
- Hacker คือ คนที่มีความรู้ ความเชี่ยวชาญเกี่ยวกับระบบเครือข่ายคอมพิวเตอร์ หรือระบบความปลอดภัย เพื่อเข้าถึงข้อมูล หรือกระทำความผิดต่าง ๆ

1.2 รูปแบบการโจมตี เช่น การผสมผสานระหว่าง มัลแวร์, Botnet และ DDos มีลักษณะคือ ผู้โจมตีจะมีเครื่องควบคุมสั่งการ เช่น เซิฟเวอร์หรือแล็บท็อป โดยจะเขียนไวรัส (มัลแวร์) ส่งไปที่เครื่องคอมพิวเตอร์ของเหยื่อ และแพร่กระจายอยู่ในเครือข่ายหรือองค์กรนั้น ๆ ฝังตัวเป็น Botnet โดยไม่รู้ตัว จนกระทั่งผู้โจมตีสั่งการไปที่เครื่องทั้งหมดเหล่านั้น เพื่อสั่งโจมตีเป้าหมายด้วยจำนวนที่มาก ที่จะทำให้ระบบ ๆ หนึ่งไม่สามารถให้บริการได้ (DDos)

2. การเข้าใจเกี่ยวกับมาตรการป้องกัน โดยอธิบายหรือแสดงให้เห็นถึงมาตรการที่สามารถใช้ป้องกันการโจมตีทางไซเบอร์ เช่น การใช้รหัสผ่านที่ปลอดภัย การป้องกันมัลแวร์ และการอัพเดตซอฟต์แวร์ เป็นต้น

2.1 การตั้งรหัสผ่านที่ปลอดภัย เพื่อให้ผู้โจมตีคาดเดาได้ยาก เช่น มีส่วนประกอบของตัวพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข อักษรพิเศษ และไม่ใช้คำที่อยู่บนพจนานุกรม หรือคำศัพท์ที่ใกล้ตัว และควรตั้งรหัสผ่านสำหรับใช้งานส่วนตัวกับใช้ที่ทำงานให้แตกต่างกัน

3. สร้างทักษะในการระมัดระวัง โดยแนะนำหรือสอนทักษะเกี่ยวกับการระมัดระวังต่อการละเมิดความปลอดภัยที่อาจเกิดขึ้น เช่น การระวังการส่งอีเมล์แฝง การตรวจสอบลิงก์ก่อนคลิก และการระวังการใช้ข้อมูลส่วนตัว เป็นต้น

4. ส่งเสริมพฤติกรรมที่ปลอดภัย ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ เช่น การสำรวจและรายงานข้อผิดพลาด การส่งรายงานการบุกรุกทางไซเบอร์ และการรายงานการโจมตีที่สำเร็จ เป็นต้น

5. สนับสนุนและการกำกับดูแลผู้ใช้งาน ในการปฏิบัติตามนโยบายและมาตรการที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

5.1 พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 คือ กฎหมายที่ตราขึ้นเพื่อให้ประเทศไทยมีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ที่กระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ มีการประสานความร่วมมือระหว่างผู้เกี่ยวข้อง พัฒนาความรู้ความสามารถของของบุคลากรและผู้เชี่ยวชาญ รวมถึงการให้ความรู้และความตระหนักถึงภัยไซเบอร์

5.2 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีสาระสำคัญ ดังนี้

- ผู้เก็บข้อมูลต้องชี้แจงข้อมูลที่จะเก็บรวบรวม และต้องได้รับอนุญาตหรือความยินยอมจากเจ้าของข้อมูลเท่านั้น จึงจะสามารถใช้และเข้าถึงข้อมูลของเจ้าของข้อมูลได้
- ผู้เก็บรวบรวมข้อมูลจะต้องรักษาข้อมูลให้เป็นความลับ
- เจ้าของข้อมูลสามารถยกเลิกสิทธิ์การเข้าถึงข้อมูลของผู้เก็บข้อมูล ลบ หรือทำลายได้

5.3 พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 เป็นกฎหมายที่ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อป้องกัน และควบคุมการกระทำผิดที่จะเกิดขึ้นจากการใช้คอมพิวเตอร์ได้ มีบทลงโทษ เช่น

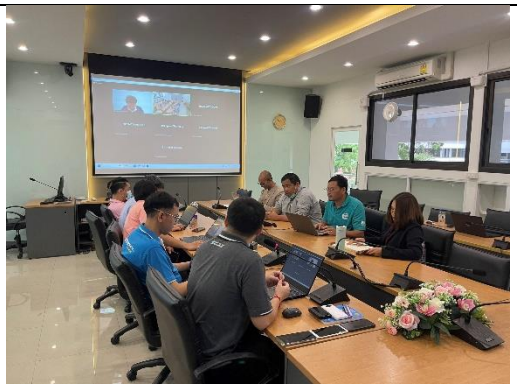
- เข้าถึงระบบคอมพิวเตอร์ที่มีการป้องกันการเข้าถึง จำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 1 แสนบาท
- ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นทำขึ้นเป็นการเฉพาะ จำคุกไม่เกิน 1 ปี ปรับไม่เกิน 2 หมื่นบาท
- เข้าถึงข้อมูลที่ไม่ใช่ของตัวเอง จำคุกไม่เกิน 2 ปี ปรับไม่เกิน 4 หมื่นบาท
- ทำข้อมูลเสียหาย แก้ไข หรือ เปลี่ยนแปลง จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาท
- ขัดขวาง ทำร้ายระบบ ดัดแปลง หรือทำลายข้อมูลผู้อื่นเสียหาย จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ
- ส่งอีเมลขายของโดยที่ลูกค้าไม่ยินดีที่จะรับ ถือเป็น Spam จำคุกไม่เกิน 2 ปี ปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ

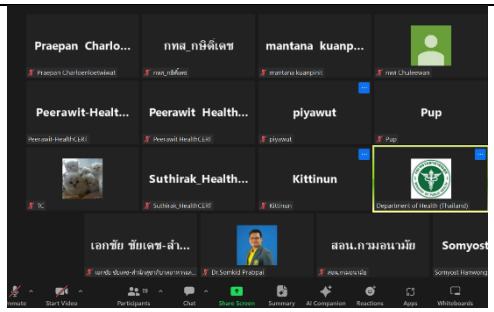
- โพสต์ข่าวปลอม การก่อการร้าย ข้อมูลลามก โดยส่งผลกระทบต่อประชาชน จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ ส่วนที่ส่งผลต่อตัวบุคคลใดบุคคลหนึ่ง จำคุกไม่เกิน 3 ปี ปรับไม่เกิน 6 แสนบาท หรือทั้งจำทั้งปรับ

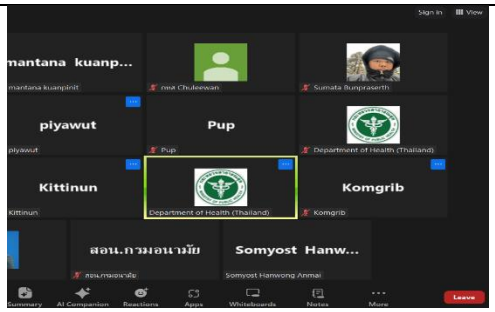
- การตัดต่อ ดัดแปลงภาพ ที่ทำให้ผู้อื่นเสียหาย และเสื่อมเสียชื่อเสียง รวมทั้งการโพสต์ภาพผู้เสียชีวิตที่ทำให้พ่อ, แม่, คู่สมรส หรือบุตรผู้ตายเสียชื่อเสียง หรือได้รับความอับอาย จำคุกไม่เกิน 3 ปี ปรับไม่เกิน 2 แสนบาท

6. เผยแพร่ความรู้และข้อมูลเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่อง ผ่านช่องทางต่าง ๆ เช่น สื่อสังคมออนไลน์ อีเมล์ และการประชาสัมพันธ์ เป็นต้น







ภาพประกอบการประชุมฯ วันที่ 9 พฤษภาคม 2567 เวลา 09.30 - 16.30 น.