มาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย
ขั้นตอนที่ 2 : จัดทำระบบเฝ้าระวังและแจ้งภัยคุกคามภัยทางไซเบอร์

จัดทำระบบเฝ้าระวังและแจ้งภัยคุกคามภัยทางไซเบอร์ โดยดำเนินการจัดทำระบบตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ เพื่อตอบสนองและยังยั้งต่อภัยคุกคามทางไซเบอร์ โดยมีการจัดเตรียมระบบ/อุปกรณ์ บุคลากร และช่องทางการสื่อสารแจ้งภัยคุกคามทางไซเบอร์ของกรมอนามัย สำหรับป้องกัน ตรวจจับ และเฝ้าระวังการบุกรุกระบบคอมพิวเตอร์และเครือข่าย รวมทั้งหน่วยงานภาครัฐที่กำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานทำหน้าที่ประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, กระทรวงสาธารณสุข โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CERT) เป็นหน่วยงานทำหน้าที่ประสานงานเฝ้าระวัง รับมือและแก้ไขภัยคุกคามทางไซเบอร์ด้านสาธารณสุข และคณะประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Anamai CIRT) ของกรมอนามัย เป็นต้น โดยมีรายละเอียด ดังนี้

๑. จัดเตรียมระบบ/อุปกรณ์สำหรับป้องกัน ตรวจจับ และเฝ้าระวังการบุกรุกระบบคอมพิวเตอร์และเครือข่าย จากภัยคุกคามทางไซเบอร์ ดังนี้

- อุปกรณ์ป้องกันความปลอดภัยด้านเครือข่าย เช่น
  - อุปกรณ์ป้องกันเครือข่าย (Firewall)
  - อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System : IPS)
  - อุปกรณ์ตรวจจับและป้องกันการโจมตีระบบเครือข่ายแบบ (DDoS)
  - อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)
  - ระบบป้องกันไวรัส (Kaspersky Antivirus Security System)
  - อุปกรณ์จัดเก็บ Log File ระบบเครือข่าย
- การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ โดยการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น
  - เทคโนโลยีการเข้ารหัสข้อมูล (Secure Socket Layer : SSL) โดยการเข้ารหัสข้อมูล เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์
  - เครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN) โดยสร้างการเชื่อมต่อเครือข่ายส่วนตัวระหว่างอุปกรณ์ต่างๆ ผ่านอินเทอร์เน็ต
- ซอฟต์แวร์เฝ้าระวังภัยคุกคามทางไซเบอร์ เช่น PRTG Network Monitor เป็นต้น
  - ระบบตรวจสอบสถานะเครือข่าย (PRTG Network Monitoring) โดยมีโปรโตคอลสำหรับมอนิเตอร์อุปกรณ์ (SNMP) และคำสั่งตรวจสอบสถานะการทำงาน UP/Down (Ping)

๒. จัดเตรียมบุคลากร เพื่อทำหน้าที่ประสานงาน เฝ้าระวัง รับมือและแก้ไขภัยคุกคามทางไซเบอร์

- ทีมรับมือ และตอบสนองต่อภัยคุกคามทางไซเบอร์มีหน้าที่รับผิดชอบในการแจ้งข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ ให้กับผู้ที่เกี่ยวข้องทั้งภายใน และภายนอกองค์กร เพื่อให้ทุกคนสามารถดำเนินการตามหน้าที่รับผิดชอบของตนเองตามกำหนดไว้ โดยมีรายละเอียด ดังนี้

ลำดับ	ผู้ที่เกี่ยวข้อง	หน้าที่รับผิดชอบ
๑	ผู้แจ้งเหตุ หรือผู้ได้รับผลกระทบ	แจ้งเหตุการณ์หรือรายงานเหตุการณ์ภัยคุกคามที่พบหรือต้องสงสัยว่าอาจจะเกิดเหตุการณ์
๒	ผู้รับแจ้งเหตุการณ์ (กองดิจิทัลเพื่อส่งเสริมสุขภาพ)	รับแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
๓	ทีมรับมือ และเฝ้าระวัง (กองดิจิทัลเพื่อส่งเสริมสุขภาพ) (เจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์)	๑. วิเคราะห์เหตุการณ์ภัยคุกคาม ๒. รับมือและตอบสนองต่อเหตุการณ์ภัยคุกคาม ๓. ให้คำปรึกษาในการป้องกัน และข้อควรระวังต่าง ๆ เกี่ยวกับเหตุการณ์ภัยคุกคาม ๔. เฝ้าระวังและวิเคราะห์การแจ้งเตือนจากอุปกรณ์ตรวจจับ ๕. ติดต่อหน่วยงานภายนอกในกรณีที่ไม่สามารถดำเนินการระงับเหตุการณ์ได้
๔	ผู้บริหาร	รับผิดชอบกำหนดนโยบาย แนวปฏิบัติ ให้ข้อเสนอแนะ และสนับสนุนงบประมาณในด้านต่าง ๆ เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

๓. ช่องทางการสื่อสารแจ้งภัยคุกคามทางไซเบอร์ของกรมอนามัย เพื่อเป็นช่องทางการรายงานเหตุการณ์ ให้ผู้ได้รับผลกระทบหรือพบเห็นเหตุการณ์ ดังนี้

- จดหมายอิเล็กทรอนิกส์ : cybersec@anamai.mail.go.th
- กลุ่มไลน์ : AnamaiCIRT
- เบอร์ติดต่อ : 0 2590 4310
- เว็บไซต์เผยแพร่ข่าวสาร : https://cybersec.anamai.moph.go.th