ตัวชี้วัด 4.21 : ระดับความสำเร็จของการเตรียมความพร้อมรัฐบาลดิจิทัลของกรมอนามัย

มีมาตรการขับเคลื่อนการดำเนินงานด้านการเตรียมความพร้อมรัฐบาลดิจิทัลของกรมอนามัย

การประชุมเชิงปฏิบัติการขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของกรมอนามัย
วันอังคารที่ 18 - 19 พฤศจิกายน 2568 เวลา ณ ห้องประชุม Sapphire 3 ชั้น 3
โรงแรมแกรนด์ริชมอนด์ จังหวัดนนทบุรี

วัตถุประสงค์

เพื่อเสริมสร้างความรู้ ความเข้าใจ และทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แก่ผู้เข้าร่วมประชุม ให้สามารถป้องกันและรับมือภัยคุกคามได้อย่างถูกต้อง ทันท่วงที รวมถึงใช้เครื่องมือเฝ้าระวังและวิเคราะห์ภัยคุกคามสมัยใหม่ได้อย่างมีประสิทธิภาพ

หน่วยงานผู้รับผิดชอบ : กลุ่มดิจิทัลเทคโนโลยีและระบบข้อมูล กองแผนงาน

จำนวนผู้เข้าร่วมประชุม : 57 คน (จาก 37 หน่วยงาน)

- ส่วนกลาง 20 แห่ง (ขาด 2 หน่วยงาน คือ กอฉ. และสถาบันเวชศาสตร์วิถีชีวิต)
- ส่วนภูมิภาค 15 แห่ง ซึ่งเป็นผู้รับผิดชอบระบบเทคโนโลยีสารสนเทศ นักวิชาการ และบุคลากรที่เกี่ยวข้องจากหน่วยงานส่วนกลางและหน่วยงานส่วนภูมิภาคของกรมอนามัย

ความเป็นมา

จากสถานการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมอนามัยระหว่างปี พ.ศ. 2566–2567 พบว่า มีความพยายามโจมตีทางไซเบอร์มากกว่า 2 ล้านเซสชั่นต่อปี หรือเฉลี่ยประมาณ 10,000 ครั้งต่อปี แม้ส่วนใหญ่จะถูกป้องกันด้วยระบบป้องกันภัยคุกคามทางไซเบอร์ของกรมอนามัย แต่ยังคงมีการโจมตีที่หลุดรอดเข้ามาเฉลี่ยปีละ 41 ครั้ง โดยมีสาเหตุมาจากการตั้งค่าระบบที่ไม่ปลอดภัย ช่องโหว่ของโปรแกรม ระบบและซอฟต์แวร์ที่ล้าสมัย รวมถึงการขาดความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

สำหรับปีงบประมาณ พ.ศ. 2568 กรมอนามัยยังคงเผชิญกับความท้าทายด้านภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง โดยถูกโจมตีมากกว่า 5 แสนครั้งต่อปี และตรวจพบการโจมตีที่หลุดรอดการป้องกันเข้ามาได้จำนวน 32 ครั้ง อีกทั้งยังตรวจพบช่องโหว่ในระบบสารสนเทศจำนวนมากในระดับ Critical และ High โดยสาเหตุหลักได้แก่ การใช้ภาษาและโปรแกรมที่เป็นรุ่นเก่า การเข้ารหัสข้อมูลที่ล้าสมัย และการขาดระบบรับส่งข้อมูลที่ปลอดภัย ซึ่งกรมอนามัยได้ดำเนินการแก้ไขด้วย 2 มาตรการ ได้แก่

1) มาตรการเชิงรับ โดยการยกระดับมาตรฐานห้องคอมพิวเตอร์แม่ข่าย (ห้อง Server) ของหน่วยงานในกรมอนามัยให้ได้ตามมาตรฐานเกณฑ์การประเมินระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือ CTAM (Cybersecurity Technical Assessment Matrix) และเกณฑ์มาตรฐานโรงพยาบาลอัจฉริยะของสำนักงานปลัดกระทรวงสาธารณสุข มาใช้ประเมิน 17 หน่วยงานของกรมอนามัยที่มีห้อง Server ซึ่งผลการประเมินส่วนใหญ่ยังไม่ผ่านเกณฑ์อยู่ระหว่างการปรับปรุงตามข้อกำหนด

2) มาตรการเชิงรุก โดยการตรวจสอบหาช่องโหว่ของระบบเว็บไซต์ภายในกรมอนามัย ด้วยการทำ VA Scan (Vulnerability Assessment Scan) เป็นประจำทุกเดือน เมื่อพบช่องโหว่ จะแจ้งให้หน่วยงานดำเนินการแก้ไข

การเสริมสร้างความเข้มแข็งด้านความมั่นคงปลอดภัยไซเบอร์ในปี 2569 กรมอนามัยได้ลงทุนจัดหาอุปกรณ์และซอฟต์แวร์ป้องกันภัยคุกคามทางไซเบอร์เพิ่มเติม ให้กับหน่วยงานส่วนกลางและส่วนภูมิภาคอาทิ อุปกรณ์ป้องกันการโจมตีขั้นสูง (Next Gen Firewall) อุปกรณ์ป้องกันเว็บไซต์ (WAF) ระบบตรวจจับพฤติกรรมผิดปกติ และระบบยืนยันตัวตนบนอุปกรณ์เคลื่อนที่ (BYOD) พร้อมทั้งเร่งปรับปรุงห้อง Server ในหน่วยงานที่ยังไม่ผ่านเกณฑ์ CTAM ซึ่งมีการปรับปรุงเกณฑ์ใหม่ในปี 2569

การจัดประชุมในครั้งนี้ ได้รับเกียรติจากวิทยากรผู้ทรงคุณวุฒิด้านความมั่นคงปลอดภัยสารสนเทศจำนวน 2 หน่วยงาน ได้แก่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และบริษัท อินฟอร์เมชั่น แอนด์ คอนซัลแตนท์ จำกัด มาให้ความรู้และแลกเปลี่ยนประสบการณ์อันเป็นประโยชน์ให้แก่ผู้เข้าร่วมประชุม