มาตรการรักษาความมั่นคงปลอดภัยไซเบอร์
ศูนย์อนามัยที่ ๙ นครราชสีมา

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มีผลบังคับใช้เพื่อป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศดังนั้นเพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที ศูนย์อนามัยที่ ๙ นครราชสีมา จึงได้จัดทำมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นแนวทางให้ถือปฏิบัติอย่างเคร่งครัด และเป็นการดำเนินการตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ โดยมีรายละเอียด ดังนี้

๑) สำรวจเว็บไซต์และระบบงานในความดูแลของหน่วยงาน และจัดทำทะเบียนชื่อเว็บไซต์และชื่อโดเมน และ IP Address เช่น ict-ops-moph.moph.go.th ๒๐๓.๑๕๗.XXXX เป็นต้น และจัดส่งสำเนาไฟล์ไปยังงานเทคโนโลยีสารสนเทศ กลุ่มจัดการเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อนำไปจัดทำทะเบียนกลางของกรมอนามัย เพื่อใช้ในการกำกับดูแลต่อไป

๒) ปิดเว็บไซต์และระบบงานที่ไม่ได้ใช้งาน รวมถึงเว็บไซต์และระบบงานที่พบความเสี่ยงทั้งหมดในทันที เพื่อลดความเสี่ยงในการถูกคุกคามทางไซเบอร์จากผู้ไม่หวังดี

๓) ดูแล Environments ทั้งหมดที่เกี่ยวข้อง ของเว็บไซต์ และอัปเดตให้ทันสมัย เช่น อัปเดตเวอร์ชันและ Patch ของระบบปฏิบัติการและขอฟต์แวร์ให้เป็นปัจจุบัน เป็นต้น

๔) ติดตั้งอุปกรณ์ป้องกันภัยคุกคามไซเบอร์ เช่น Firewall, Web Application Firewall และ Antivirus เป็นต้น พร้อมตั้งค่าให้ถูกต้อง เหมาะสมกับระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน

๕) เฝ้าระวังภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง โดยต้องจัดให้มีเจ้าหน้าที่ปฏิบัติงานเป็นประจำอย่างน้อย ๑ คน และต้องสามารถประสานงานกับ งาน IT ของศูนย์อนามัยที่ ๙ นครราชสีมา กรมอนามัยและ Health CERT สป.สธ. ได้ตลอดเวลา

๖) ก่อนเผยแพร่ข้อมูลส่วนบุคคลในทุกช่องทางทั้งระบบอินทราเน็ตและอินเทอร์เน็ต จะต้องได้รับความเห็นชอบหรืออนุญาต (อย่างมีหลักฐาน) จากผู้บริหารสูงสุดของหน่วยงาน

๗) เว็บไซต์และระบบงาน ควรใช้ชื่อโดเมนของกระทรวงสาธารณสุข (xxx.anamai.moph.goth) โดยแจ้งความประสงค์เป็นหนังสือราชการถึงงาน IT ของศูนย์อนามัยที่ ๙ นครราชสีมา กรมอนามัย

๘) ตรวจสอบรายการปัจจัยเสี่ยงที่ทำให้เกิดช่องโหว่ทางไซเบอร์ ดังต่อไปนี้ หากพบให้จัดการปิดช่องโหว่ทันทีหรือโดยเร็วที่สุด

๘.๑ มีการอัปโหลดไฟล์ที่มีความสำคัญขึ้นบนหน้าเว็บไซต์ทั้งภายใต้โดเมน (anamai.moph.go.th) และภายนอก (Development Platform ต่างๆ เช่น github) ทำให้ผู้โจมตีใช้ประโยชน์ได้ เช่น ไฟล์ที่ประกอบด้วยUsername Password สำหรับเข้าใช้งานระบบ, Source code ของระบบ Token ในการยืนยันตัวตน

๘.๒ ขาดการอัปเดตซอฟต์แวร์ที่ใช้งานให้เป็นเวอร์ชันปัจจุบัน

๘.๓ มี CMS Plugins ที่ไม่ได้ใช้งานแล้วแต่ยังไม่ถอนการติดตั้ง

๘.๔ ขาดการทำ Data...

๘.๔ ขาดการทำ Data Encryption เพื่อการรับ-ส่งข้อมูลสำคัญทำได้จากคนที่มี Key เท่านั้น

๘.๕ ไม่มีการปิดกั้นการ exposed ของ website configuration, database configuration, website directory หรือเปิดให้เข้าถึงไฟล์ได้จากอินเทอร์เน็ตโดยไม่มีการตรวจสอบ เช่น เปิดหน้า Index Directory ไว้ ทำให้เห็นไฟล์ต่างๆ

๘.๖ ไม่ได้กำหนด IP Address ที่จะเข้าถึง Service จากระยะไกลที่มีความอ่อนไหว เช่น Database และ Network Protocol ต่าง ๆ

๘.๗ ไม่ได้กำหนด Rate-Limitation ในการเข้าถึง Service ว่าหากเกิด Connection failedบ่อยๆ จะต้องถูกปิดกั้น

๘.๘ ไม่มีการทำตรวจสอบ User Input ทำให้สามารถพัฒนาเป็นช่องโหว่ที่ใช้โจมตีได้ เช่น SQL Injection, XSS Attack

๘.๙ ไม่มีการปิด Error ที่ระบบตอบกลับ ทำให้ผู้โจมตีตรวจสอบได้ว่า Payload ที่ใช้สามารถทำงานได้หรือไม่

๘.๑๐ เปิดให้เชื่อมต่อ Database จากสาธารณะ เช่น เปิด Port ๓๓๐๖ โดยไม่ผ่าน VPN

๘.๑๑ มีการแชร์ไฟล์ที่มีข้อมูลส่วนบุคคลในพื้นที่สาธารณะ (Public File Sharing) เช่น google drive , One Drive โดยเข้ารหัสไฟล์ หรือแชร์เฉพาะบุคคล

๘.๑๒ ขาดการตรวจสอบ Username และ Permission บนระบบที่อยู่ภายใต้การดูแลให้ถูกต้อง หากพบความผิดปกติ ควรแก้ไขโดยทันที

๙) กำหนดช่องทางติดต่อ

๑.ระดับกรม

โทรศัพท์ ๐๒-๕๙๐๔๓๑๐

อีเมล: dhealth@anamai.mail.go.th

เว็บไซต์: https://ict.anamai.moph.go.th

Line Official: @slz๐๗๔๐v

๒.ระดับกระทรวง Health CERT

โทรศัพท์ ๑๘ ๓๐๖๔ ๙๙๕๖๗, ๐ ๒๕๕๙๐ ๑๑๖๖๙, ๐ ๒๕๕๙๐ ๑๒๐๐

อีเมล: health-cirt@moph.go.th

Line Official: @health-cirt

เว็บไซต์แจ้งเหตุการณ์ใขเบอร์: https://health-cirt.moph.th

เว็บไซต์เผยแพร่ประชาสัมพันธ์ข้อมูลข่าวสารทางไซเบอร์: https://cyber.moph.go.th/