



แนวทางในการป้องกันและจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ หน่วยบริการในจังหวัดพิจิตร

ปัจจุบันปัญหาเรื่องภัยคุกคามทางไซเบอร์ (Cyber Security) ยังคงเกิดขึ้นอย่างต่อเนื่องตามเทคโนโลยีที่ทันสมัย และมีการปรับเปลี่ยนวิธีการหรือมีความรุนแรงเพิ่มมากขึ้น ดังนั้นหน่วยงานจึงจำเป็นต้องตระหนักถึงความสำคัญ การเฝ้าระวัง และการปฏิบัติให้ถูกต้องตามแนวทางในการจัดการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อเป็นการป้องกันและรับมือจากภัยคุกคามที่เกิดขึ้นได้อย่างทันท่วงที

สำนักงานสาธารณสุขจังหวัดพิจิตรจึงได้จัดทำแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยอาศัยอำนาจตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒, พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อเป็นแนวทางให้หน่วยบริการในจังหวัดพิจิตรปฏิบัติตามอย่างเคร่งครัด ดังนี้

๑. ตรวจสอบและจำกัดสิทธิของบัญชีผู้ใช้ให้สอดคล้องกับความจำเป็นในการเข้าถึงระบบและฐานข้อมูลในระบบได้แก่ HDC, HOSxP, MOPH-IC, MOPH PHR และระบบอื่นๆ ที่มีการเข้าถึงข้อมูลส่วนบุคคล
๒. เพิ่มมาตรการป้องกันเว็บไซต์สำคัญด้วยระบบป้องกันการโจมตีของไวรัส Web Application, Firewall หรือ DDoS Protection
๓. เจ้าหน้าที่ของหน่วยงานจะต้องมีความระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงข้อความ โพสต์ จาก Social Media
๔. หากพบความผิดปกติที่สงสัยว่าระบบถูกโจมตี เช่น ไม่สามารถเข้าใช้งานระบบ/เว็บไซต์ได้หรือมีความล่าช้าผิดปกติควรตรวจสอบ Log การ login ย้อนหลังทุกๆ เดือน
๕. หลีกเลี่ยงการเชื่อมต่ออินเทอร์เน็ตภายนอกกับ HIS ของหน่วยบริการ
๖. โรงพยาบาลทุกแห่งมีแนวทางการจัดการความเสี่ยง (Risk Management) ด้าน Cyber Security
๗. หน่วยบริการทุกแห่งมีระบบ Security ในการป้องกันความปลอดภัยของข้อมูลตามเกณฑ์ดังนี้
 - ๗.๑ มีนโยบาย ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบข้อมูลสารสนเทศ เช่น การ Login ด้วย User และจำกัดสิทธิการเข้าถึงข้อมูลที่จำเป็น, มีการป้องกันการเข้าถึงเว็บไซต์ที่ไม่ปลอดภัย เป็นต้น
 - ๗.๒ มีการสำรองข้อมูลของ Server และ Client เป็นประจำทุกวัน
 - ๗.๓ หน่วยบริการทุกแห่งมีระบบ Antivirus ของ Server และ Client
 - ๗.๓ โรงพยาบาลทุกแห่งมีระบบ Firewall เพื่อตรวจจับการบุกรุกของระบบเครือข่ายดังนี้
 - รพ. ระดับ S และ M๒ เกณฑ์ขั้นต่ำคือ Next-generation Firewall (Firewall ขั้นสูงสามารถรักษาความปลอดภัยจากเครือข่ายอื่นๆ และตรวจจับการบุกรุกทั้งจากการรับ - ส่งข้อมูล, IP Address และแอปพลิเคชันต่างๆ ที่สามารถรับ - ส่งข้อมูลจากภายนอกได้ เช่น อีเมล เป็นต้น)
 - รพ. ระดับ F๒ และ F๓ เกณฑ์ขั้นต่ำคือ Entry Level Firewall (Firewall ที่ตรวจสอบการบุกรุกจากช่องทางการรับ - ส่งข้อมูล, IP Address หรือป้องกันเพียงบางเครือข่ายเท่านั้น)
๘. หน่วยบริการมีระบบ Log เก็บข้อมูลติดต่อภายนอก

๙. การจัดการปัจจัยเสี่ยง ที่ทำให้เกิดช่องโหว่ทาง Cyber อื่นๆ ที่อาจนำไปสู่ความผิด PDPA
- ๙.๑ หลีกเลี่ยงการอัปโหลดไฟล์ที่มีความสำคัญขึ้นบนหน้าเว็บไซต์ทั้งภายใต้โดเมน (moph.go.th) และภายนอก (Development Platform ต่างๆ เช่น github) ที่ทำให้ผู้โจมตีใช้ประโยชน์ได้ เช่น ไฟล์ที่ประกอบด้วย Username Password สำหรับเข้าใช้งานระบบ, Source code ของระบบ
- ๙.๒ อัปเดตซอฟต์แวร์ที่ใช้งานให้เป็นเวอร์ชันปัจจุบัน
- ๙.๓ ถอนการติดตั้งแพลตฟอร์มหรือโปรแกรมเสริมที่ใช้จัดการเว็บไซต์และฐานข้อมูล (CMS Plugins) ที่ไม่ได้ใช้งานแล้ว
- ๙.๔ การเข้ารหัสข้อมูลสำคัญเฉพาะคนที่มสิทธิเข้าถึงเท่านั้น เช่น เลขประจำตัวประชาชน
- ๙.๕ หลีกเลี่ยงการเปิดให้เข้าถึงไฟล์ได้จากอินเทอร์เน็ตโดยไม่มีการตรวจสอบ เช่น เปิดหน้า Index Directory ไว้ ทำให้เห็นไฟล์ต่างๆ
- ๙.๖ กำหนด IP Address ที่จะเข้าถึง Service ที่มีความอ่อนไหว เช่น MySQL, SSH
- ๙.๗ กำหนด Rate-Limitation ในการเข้าถึง Service ว่าหากเกิด Connection failed หลายครั้ง จะต้องถูกปิดกั้น
- ๙.๘ มีการตรวจสอบ User Input เช่น SQL Injection, XSS Attack ที่ทำให้สามารถพัฒนาเป็นช่องโหว่ ที่ใช้โจมตีได้
- ๙.๙ ปิดกั้นการ exposed ของ website configuration, database configuration, website directory
- ๙.๑๐ หลีกเลี่ยงการเปิดให้เชื่อมต่อ port 3306 จากสาธารณะ โดยไม่ผ่าน VPN
- ๙.๑๑ หลีกเลี่ยงการแชร์ข้อมูลส่วนบุคคลในพื้นที่สาธารณะเช่น google drive, OneDrive โดยไม่เข้ารหัสไฟล์ หรือแชร์เฉพาะบุคคล เป็นต้น
- ๙.๑๒ ตรวจสอบ Username และ Permission บนระบบที่อยู่ภายใต้การดูแลให้ถูกต้อง หากพบความผิดปกติ ควรแก้ไขโดยทันที
๑๐. การเผยแพร่ข้อมูล โดยเฉพาะข้อมูลส่วนบุคคล ควรได้รับความเห็นชอบ (อย่างมีหลักฐาน) จากผู้บริหารสูงสุดของหน่วยงานก่อนเผยแพร่สู่สาธารณะ (ทั้ง Intranet และ Internet)

สำนักงานสาธารณสุขจังหวัดพิจิตร

๔ เมษายน ๒๕๖๖