ตัวชี้วัด ๔.๒๐ : ระดับความสำเร็จของการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย

ระดับที่ ๔ Output ผลผลิต

มีผลลัพธ์ตรงเป้าหมายเป็นสัดส่วนตามระยะเวลา โดยดำเนินการแล้วเสร็จภายในเดือนกุมภาพันธ์ ๒๕๖๙

๔.๑ มีจำนวนการละเมิดความปลอดภัยทางไซเบอร์ (Security Breaches) ของกรมอนามัยลดลงจาก ๒๕ ครั้ง/ปี เหลือไม่เกิน ๑๓ ครั้ง/ปี (ลดลงร้อยละ ๕๐) (รอบที่ ๑ : ๕ เดือนแรก)

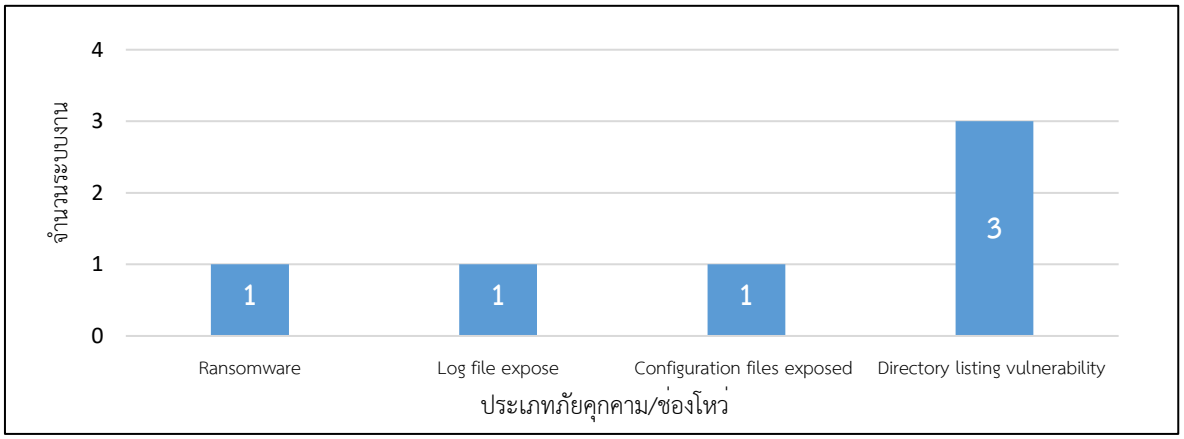
๔.๑.๑ แนวทางการประเมิน

๑) เกณฑ์คะแนน

คะแนน	การละเมิดความปลอดภัย (ครั้ง)
๐.๒	>=๒๐
๐.๔	๑๘-๑๙
๐.๖	๑๖-๑๗
๐.๘	๑๔-๑๕
๑.๐	<=๑๓

๔.๑.๒ ผลลัพธ์ของการประเมิน

กองแผนงาน ได้ตรวจพบหรือได้รับแจ้งเหตุภัยคุกคาม/ช่องโหว่ของระบบงาน ระบบเครือข่าย และเว็บไซต์หน่วยงานในสังกัดกรมอนามัย ในเดือนตุลาคม - กุมภาพันธ์ ๒๕๖๙ จึงสรุปได้ว่า จำนวนภัยคุกคามหรือช่องโหว่ที่พบมีทั้งหมด ๖ เรื่อง ดังนี้



รูปที่ ๑ แสดงจำนวนภัยคุกคาม/ช่องโหว่ที่ตรวจพบ เดือนตุลาคม - กุมภาพันธ์ ๒๕๖๙

จากรูปที่ ๑ สรุปได้ว่า ประเภทภัยคุกคาม/ช่องโหว่ ตรวจพบ ดังนี้

๑. แรนซัมแวร์ (Ransomware) หรือ "มัลแวร์เรียกค่าไถ่" คือซอฟต์แวร์ประสงค์ร้ายที่แฮกเกอร์ใช้ล็อกหรือเข้ารหัสไฟล์ข้อมูลในคอมพิวเตอร์/เครือข่าย ทำให้เจ้าของเข้าใช้งานไม่ได้ แล้วเรียกร้องเงิน จำนวน ๑ ระบบงาน

๑.๑. ระบบงาน/เว็บไซต์ : hpc11.go.th

หน่วยงานผู้ดูแลระบบ: ศูนย์อนามัยที่ ๑๑ นครศรีธรรมราช

ระบบงาน : Happy body HPC11

จำนวนในการตรวจพบมัลแวร์เรียกค่าไถ่ : ๑ ครั้ง

สถานะ : ดำเนินการแก้ไขแล้ว

รายละเอียด : ได้รับแจ้งจาก ศูนย์อนามัยที่ ๑๑ นครศรีธรรมราช แจ้งการโจมตีระบบเว็บไซต์ hpc11.go.th ของศูนย์อนามัยที่ ๑๑ นครศรีธรรมราช ซึ่งเป็นลักษณะ Ransomware ส่งผลให้ไฟล์ภายในระบบมีการเปลี่ยนนามสกุล และตรวจพบไฟล์ลักษณะเป็นข้อความแสดงการบุกรุก (เช่น ไฟล์ที่มีข้อความ “hack by ...”) ทั้งนี้ ยังไม่สามารถยืนยันได้ว่ามีข้อความหรือไฟล์อื่นใดจากผู้โจมตีหลงเหลืออยู่ในระบบหรือไม่ เนื่องจากผู้พัฒนาของระบบได้ลบส่วนของข้อความดังกล่าวไปแล้วส่งผลให้ข้อมูลหลักฐานบางส่วนอาจสูญหาย ปัจจุบันยังไม่สามารถระบุได้ชัดเจนว่าการโจมตีดังกล่าวเป็นฝีมือของกลุ่มใด อยู่ระหว่างการรวบรวมข้อมูลเพื่อการวิเคราะห์เชิงลึกโดยหน่วยงานที่เกี่ยวข้อง

๒. การเปิดเผยไฟล์บันทึก (Log file expose) คือ ความเสี่ยงด้านความปลอดภัยที่เกิดขึ้นเมื่อไฟล์บันทึกการทำงานของระบบ (Log files) ที่เก็บข้อมูลละเอียด จำนวน ๑ ระบบงาน

๒.๑. ระบบงาน/เว็บไซต์ : https://envplan.anamai.moph.go.th/pages/pages.log

หน่วยงานผู้ดูแลระบบ: สำนักอนามัยสิ่งแวดล้อม

ระบบงาน : ระบบฐานข้อมูลกลางกรมอนามัย

จำนวนในการตรวจพบการเปิดเผยไฟล์ : ๑ ครั้ง

สถานะ : ดำเนินการแก้ไขเรียบร้อย

รายละเอียด : เนื่องจากการตรวจสอบของกองแผนงาน พบความเสี่ยงด้านความปลอดภัยที่เกิดขึ้นเมื่อไฟล์บันทึกการทำงานของระบบ (Log files) ที่เก็บข้อมูลละเอียด เช่น IP address, พฤติกรรมการใช้งาน, ข้อผิดพลาดของระบบ, หรือข้อมูลการเข้าสู่ระบบ ถูกเปิดเผยหรือเข้าถึงโดยไม่ได้รับอนุญาต ส่งผลให้ข้อมูลส่วนบุคคลหรือข้อมูลสำคัญรั่วไหล ทำให้เสี่ยงต่อการถูกโจมตีทางไซเบอร์

๓. ไฟล์การตั้งค่าถูกเปิดเผย (Configuration files exposed) คือช่องโหว่ความปลอดภัยที่ไฟล์สำคัญหรือไฟล์ตั้งค่าฐานข้อมูล ถูกเข้าถึงได้โดยบุคคลภายนอกผ่านอินเทอร์เน็ต จำนวน ๑ ระบบงาน

๓.๑. ระบบงาน/เว็บไซต์ : https://healthreligions.anamai.moph.go.th/sitemap.xml

หน่วยงานผู้ดูแลระบบ: สำนักอนามัยผู้สูงอายุ

ระบบงาน : ระบบพระสงฆ์กับการพัฒนาสุขภาวะ

สถานะ : ดำเนินการแก้ไขเรียบร้อย

จำนวนในการตรวจพบการเปิดเผยไฟล์ : ๑ ครั้ง

รายละเอียด : เนื่องจากการตรวจสอบของกองแผนงาน พบช่องโหว่ความปลอดภัยที่ไฟล์สำคัญหรือไฟล์ตั้งค่าฐานข้อมูล ถูกเข้าถึงได้โดยบุคคลภายนอกผ่านอินเทอร์เน็ต เกิดจากการตั้งค่าเว็บเซิร์ฟเวอร์ผิดพลาด หรือการเผลออัปโหลดข้อมูลสำคัญขึ้น Git repository สาธารณะ ทำให้ผู้โจมตีทราบรหัสผ่านและโครงสร้างระบบ

๔. Directory listing vulnerability คือ ช่องโหว่ด้านความปลอดภัยที่เกิดจากการตั้งค่าเว็บเซิร์ฟเวอร์ (Web Server) ไม่ถูกต้อง จำนวน ๓ ระบบงาน

๔.๑. ระบบงาน/เว็บไซต์ https://envplan.anamai.moph.go.th/pages/?pg=

หน่วยงานผู้ดูแลระบบ : สำนักอนามัยสิ่งแวดล้อม

ระบบงาน : โปรแกรมติดตามผลการดำเนินงานสำนักอนามัยสิ่งแวดล้อม

จำนวนในการตรวจพบช่องโหว่ : ๒ ครั้ง

สถานะ : ดำเนินการแก้ไขเรียบร้อย (อยู่ระหว่างเฝ้าระวัง)

รายละเอียด : เนื่องจากการตรวจสอบของกองแผนงาน พบช่องโหว่ด้านความปลอดภัยที่เกิดจากการตั้งค่าเว็บเซิร์ฟเวอร์ (Web Server) ไม่ถูกต้อง ทำให้เมื่อผู้ใช้งานเข้าชม URL ของไดเรกทอรีที่ไม่มีไฟล์หน้าแรก (เช่น index.html) เซิร์ฟเวอร์จะแสดงรายการไฟล์และโฟลเดอร์ทั้งหมดภายในไดเรกทอรีนั้นออกมาในรูปแบบรายการ (List) แทนที่จะแจ้งข้อผิดพลาดหรือแสดงหน้าว่าง

๔.๒. ระบบงาน/เว็บไซต์ **https://backenddc.anamai.moph.go.th/coverpage/**

หน่วยงานผู้ดูแลระบบ : กองแผนงาน

ระบบงาน : ระบบฐานข้อมูลกลางกรมอนามัย

จำนวนในการตรวจพบช่องโหว่ : ๑ ครั้ง

สถานะ : ดำเนินการแก้ไขเรียบร้อย

รายละเอียด : เนื่องจากการตรวจสอบของกองแผนงาน พบช่องโหว่ด้านความปลอดภัยที่เกิดจากการตั้งค่าเว็บเซิร์ฟเวอร์ (Web Server) ไม่ถูกต้อง ทำให้เมื่อผู้ใช้งานเข้าชม URL ของไดเรกทอรีที่ไม่มีไฟล์หน้าแรก (เช่น index.html) เซิร์ฟเวอร์จะแสดงรายการไฟล์และโฟลเดอร์ทั้งหมดภายในไดเรกทอรีนั้นออกมาในรูปแบบรายการ (List) แทนที่จะแจ้งข้อผิดพลาดหรือแสดงหน้าว่าง

Output ผลผลิตของมีจำนวนการละเมิดความปลอดภัยทางไซเบอร์ (Security Breaches) ของกรมอนามัย ในเดือนตุลาคม - กุมภาพันธ์ ๒๕๖๙ จำนวน ๖ ครั้ง ซึ่งไม่เกิน ๑๓ ครั้ง/ปี และมีการดำเนินการแก้ไขเรียบร้อยแล้วภายใน ๒๔ ชั่วโมง ตรวจสอบไม่พบการถูกละเมิดที่ไม่ก่อให้เกิดความเสียหายต่อระบบงาน ระบบเครือข่าย และเว็บไซต์หน่วยงานกรมอนามัย จึงได้ คะแนน ๑ คะแนน