ตัวชี้วัด 4.19 : ระดับความสำเร็จของการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย

ระดับที่ 5 Outcome ผลลัพธ์ของตัวชี้วัด

มีผลลัพธ์ตรงเป้าหมายเป็นสัดส่วนตามระยะเวลา โดยดำเนินการแล้วเสร็จภายในเดือนกรกฎาคม 2568

5.1 มีจำนวนการละเมิดความปลอดภัยทางไซเบอร์ (Security Breaches) ของกรมอนามัยลดลงจาก 32 ครั้ง/ปี เหลือไม่เกิน 25 ครั้ง/ปี (ลดลงร้อยละ 20) (รอบที่ 2 : 5 เดือนหลัง) (0.5 คะแนน)

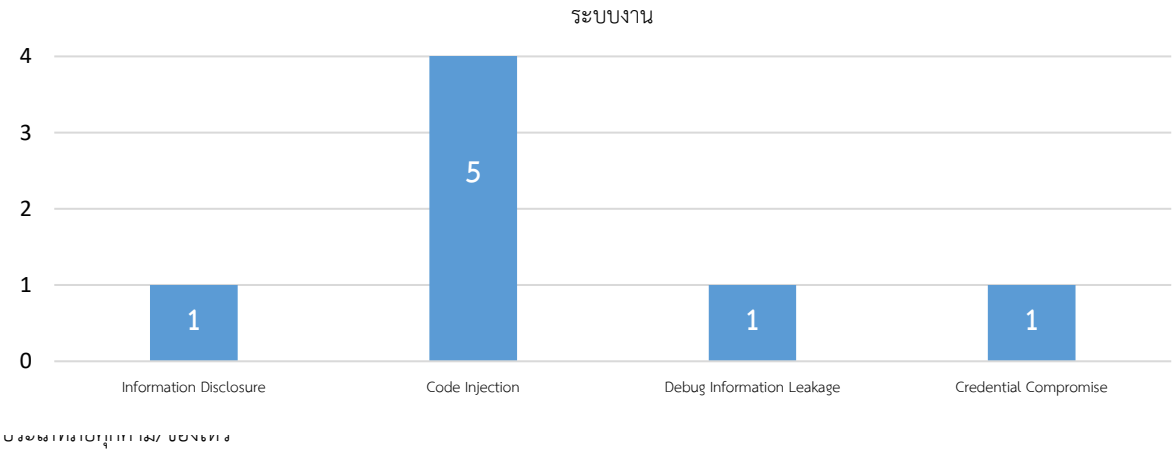
5.1.1 แนวทางการประเมิน

1) เกณฑ์คะแนน

คะแนน	การละเมิดความปลอดภัย (ครั้ง)
0.2	>=19
0.4	17-18
0.6	15-16
0.8	13-14
1.0	<=12

5.1.2 ผลลัพธ์ของการประเมิน

กองแผนงาน ได้ตรวจพบหรือได้รับแจ้งเหตุภัยคุกคาม/ช่องโหว่ ของระบบงาน ระบบเครือข่าย และเว็บไซต์หน่วยงานในสังกัดกรมอนามัย ในเดือนเมษายน - กรกฎาคม 2568 จึงสรุปได้ว่า จำนวนภัยคุกคามหรือช่องโหว่ที่พบมีทั้งหมด 8 เรื่อง ดังนี้



รูปที่ 1 แสดงจำนวนภัยคุกคาม/ช่องโหว่ที่ตรวจพบ เดือนเมษายน - กรกฎาคม 2568

จากรูปที่ 1 สรุปได้ว่า ประเภทภัยคุกคาม/ช่องโหว่ ตรวจพบ ดังนี้

- ลำดับ 1 Information Disclosure - Personal Data Exposure คือแสดงข้อมูลส่วนบุคคลของผู้ใช้บนระบบโดยไม่ได้ตั้งใจ

    1. ระบบงาน/เว็บไซต์ **https://hpci.anamai.moph.go.th/hl/MomChild/RptChEv.aspx**
       หน่วยงานผู้ดูแลระบบ: ศูนย์อนามัยที่ 9
       สถานะ : ดำเนินการแก้ไขเรียบร้อย

- ลำดับ 2 Debug Information Leakage เผยแพร่ข้อมูล Database Query Debug บนเว็บไซต์ production

    1. ระบบงาน/เว็บไซต์ : https://healthtemple.anamai.moph.go.th/auth/login
       ระบบข้อมูลวัดส่งเสริมสุขภาพและพระคิลานุปัฏฐาก
       หน่วยงานผู้ดูแลระบบ: สำนักอนามัยผู้สูงอายุ
       สถานะ : ดำเนินการแก้ไขเรียบร้อย

- ลำดับ 3 Code Injection via PHP Vulnerability มีการแฝงข้อมูลเว็บพนันบนเว็บไซต์

    1. หน่วยงานผู้ดูแลระบบ: กองแผนงาน
       จำนวนในการตรวจพบเว็บพนัน : 5 ครั้ง
       สถานะ : ดำเนินการแก้ไขเรียบร้อย (เฝ้าระวัง)
       รายละเอียด : เนื่องจากระบบมีช่องโหว่ในการ Version PHP ที่มีช่องโหว่จากเทคโนโลยีการโจมตีรูปแบบใหม่ ๆ ทำให้มีการแอบแฝง Link หรือข้อความเว็บพนันบนเว็บไซต์ในหน่วยงาน หลาย ๆ หน่วยงาน โดยเป็น Mini Size ของ Website 4.0 ที่กองแผนดูแล

- ลำดับ 4 Credential Compromise via Malware ข้อมูล User Password รั่วไหล

    1. ระบบงาน/เว็บไซต์ Web Application ภายในกรมอนามัย
       หน่วยงานผู้ดูแลระบบ: หน่วยงานสังกัดกรมอนามัย
       สถานะ : ดำเนินการแก้ไขแล้ว (อยู่ระหว่างดำเนินการจัดทำแนวทางการป้องกันเพิ่มเติม)
       เหตุการณ์: ได้รับแจ้งจาก ทีม CIRT เรื่องการหลุดของข้อมูล User Password ในหลายเว็บไซต์ของหน่วยงานสังกัดกรมอนามัย และทุกหน่วยงานสังกัดกระทรวงสาธารณสุข ปัจจัยหลักเกิดจากการใช้ Software ที่ไม่มีลิขสิทธิ์ หรือผิดลิขสิทธิ์ส่งผลให้มี Malware ฝังตัวและมีการจัดเก็บข้อมูล User Password ระบบงาน และนำออกจากผู้ใช้

Outcome ผลลัพธ์ของจำนวนการละเมิดความปลอดภัยทางไซเบอร์ (Security Breaches) ของกรมอนามัย จำนวน 8 ครั้ง ได้ 0.5 คะแนน ซึ่งน้อยกว่า 12 ครั้ง ในรอบ 5 เดือนหลัง

5.2 ร้อยละความสำเร็จในการกู้คืนระบบงานกองแผนงานให้พร้อมใช้งานภายใน 24 ชั่วโมง หลังจากตรวจพบการถูกละเมิดความปลอดภัยทางไซเบอร์ (Security Breaches) จากจำนวนระบบทั้งหมด 54 ระบบ (รอบที่ 2 : 5 เดือนหลัง) 0.5 คะแนน

5.2.1 แนวทางการประเมิน

1) เกณฑ์คะแนน

คะแนน	เป้าหมาย (ร้อยละ)
0.1	<=80
0.2	80-84.99
0.3	85-89.99
0.4	90-94.99
0.5	>=95 ขึ้นไป

2) สูตรคำนวณการดำเนินงานตามตัวชี้วัด

$$\text{ร้อยละความสำเร็จในการกู้คืนระบบงานกองแผนงาน} = \frac{(\text{จำนวนครั้งที่กู้คืนระบบสำเร็จภายใน } 24 \text{ ชม.})}{(\text{จำนวนครั้งที่ถูกละเมิดความปลอดภัยทางไซเบอร์})} \mathbf{x} 100$$

Outcome ผลลัพธ์ของร้อยละความสำเร็จในการกู้คืนระบบงานกองแผนงานให้พร้อมใช้งานภายใน 24 ชั่วโมง หลังจากตรวจพบการถูกละเมิดความปลอดภัยทางไซเบอร์ (Security Breaches) พบว่า กองแผนงานไม่มีระบบงานที่ต้องดำเนินการกู้คืนให้พร้อมใช้งานภายใน 24 ชม. ได้ คะแนน 0.5 คะแนน

ทั้งนี้ ในช่วงเดือนเมษายน – กรกฎาคม 2568 กองแผนงาน ไม่พบเหตุการณ์การถูกละเมิดความปลอดภัยทางไซเบอร์ ที่ส่งผลกระทบต่อระบบงานแต่อย่างใด ส่งผลให้ ไม่มีข้อมูลที่ถูกละเมิด และสามารถ ควบคุมสถานการณ์ได้อย่างทันท่วงที สะท้อนว่า หน่วยงานมีความพร้อมและประสิทธิภาพในการป้องกันการละเมิดด้านความปลอดภัยทางไซเบอร์ ได้อย่างมีประสิทธิภาพ