ตัวชี้วัด 4.21 : ระดับความสำเร็จของมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

5. Outcome ผลลัพธ์ของตัวชี้วัดร้อยละการรายงานภัยคุกคามทางไซเบอร์

มีผลลัพธ์ตรงเป้าหมายเป็นสัดส่วนตามระยะเวลา โดยดำเนินการแล้วเสร็จภายในวันที่ 31 กรกฎาคม 2567

5.2 ร้อยละของการช่วยเหลือให้หน่วยงานในสังกัดกรมอนามัย ตามมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย (ร้อยละ 80) (0.7) (รอบที่ 2: 5 เดือนหลัง)

5.2.1 แนวทางการประเมิน

1) เกณฑ์คะแนน

คะแนน	เป้าหมาย (ร้อยละ)
0.1	<= 30
0.2	31 - 40
0.3	41 - 50
0.4	51 - 60
0.5	61 - 70
0.6	71 - 80
0.7	> 80 ขึ้นไป

2) สูตรคำนวณ

$$\text{ร้อยละความสำเร็จของการแก้ไขภัยคุกคามทางไซเบอร์} = \frac{(100 \text{ x จำนวนการช่วยเหลือให้หน่วยงานในสังกัดกรมอนามัยตามมาตรการฯ})}{(\text{จำนวนที่ตรวจพบภัยคุกคามทางไซเบอร์ทั้งหมด})}$$

5.2.2 ผลลัพธ์ของการประเมิน

ร้อยละความสำเร็จของการแก้ไขภัยคุกคามทางไซเบอร์ ระหว่างเดือนมีนาคม 2566 – กรกฎาคม 2567 เท่ากับเกณฑ์เป้าหมาย (ร้อยละ) คือ > 80 ขึ้นไป โดยสามารถดำเนินการได้ ร้อยละ 100 ซึ่งดำเนินการได้ครบทุกหน่วยงานในสังกัดกรมอนามัยที่เกิดภัยคุกคามทางไซเบอร์

Outcome ผลลัพธ์ของตัวชี้วัดร้อยละของการช่วยเหลือให้หน่วยงานในสังกัดกรมอนามัย ตามมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย ได้ 0.7 คะแนน

5.2.3 การดำเนินงานการช่วยเหลือให้หน่วยงานในสังกัดกรมอนามัย ตามมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย

1) สูตรคำนวณของการดำเนินงานตามตัวชี้วัด

$$\text{ร้อยละความสำเร็จของการแก้ไขภัยคุกคามทางไซเบอร์} = \frac{(100 \text{ x จำนวนการช่วยเหลือให้หน่วยงานในสังกัดกรมอนามัยตามมาตรการฯ})}{(\text{จำนวนที่ตรวจพบภัยคุกคามทางไซเบอร์ทั้งหมด})}$$

$$= \frac{(100 \text{ x } 19)}{(19)}$$

$$= 100$$

ร้อยละของการช่วยเหลือให้หน่วยงานในสังกัดกรมอนามัย ตามมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย ระหว่างเดือนมีนาคม 2566 – กรกฎาคม 2567 เท่ากับเป้าหมาย (ร้อยละ) คือ 100

2) ตารางรายงานข้อมูลจำนวนการช่วยเหลือให้หน่วยงานในสังกัดกรมอนามัย ตามมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย

ลำดับ	การช่วยเหลือให้หน่วยงานในสังกัดกรมอนามัย ตามมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย (เดือน)	จำนวนที่ตรวจพบภัยคุกคามทางไซเบอร์ทั้งหมด (ครั้ง)	จำนวนการช่วยเหลือให้หน่วยงานในสังกัดกรมอนามัย ตามมาตรการฯ (ครั้ง)
1	การช่วยเหลือให้หน่วยงานในสังกัดกรมอนามัย ตามมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย เดือนมีนาคม 2567	6	6
2	การช่วยเหลือให้หน่วยงานในสังกัดกรมอนามัย ตามมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย เดือนเมษา 2567	6	6
3	การช่วยเหลือให้หน่วยงานในสังกัดกรมอนามัย ตามมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย เดือนพฤษภาคม 2567	1	1
4	การช่วยเหลือให้หน่วยงานในสังกัดกรมอนามัย ตามมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย เดือนมิถุนายน 2567	3	3
5	การช่วยเหลือให้หน่วยงานในสังกัดกรมอนามัย ตามมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย เดือนกรกฎาคม 2567	3	3
รวม		19	19

3) หลักฐานการช่วยเหลือให้หน่วยงานในสังกัดกรมอนามัย ตามมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย

คำแนะนำในการปฏิบัติเพื่อลดความเสี่ยงที่จะถูกโจมตีระบบงาน/เว็บไซต์โดยทั่วไป สำหรับผู้ดูและระบบ

หน่วยงานที่รับผิดชอบระบบงาน/เว็บไซต์ จะต้องดำเนินการตรวจสอบช่องโหว่อยู่เสมอ หากตรวจพบควรดำเนินการแก้ไข เพื่อไม่ให้ผู้ไม่หวังดีใช้เป็นที่ระหำความเสียต่อไป โดยผู้ดูและระบบควรแจ้งเปลี่ยนรหัสผ่านของผู้ใช้งานทั้งหมด ตรวจสอบการกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงข้อมูล ลบสิ่งที่ไม่ได้ใช้งาน และให้ดำเนินการตรวจสอบช่องโหว่เพื่อเฝ้าระวังป้องกันการโจมตีต่อไป

ในการพัฒนาหรือตรวจสอบช่องโหว่ของระบบงาน/เว็บไซต์ ควรปฏิบัติตามคำแนะนำจาก OWASP TOP 10 Project (OWASP เป็นองค์กรที่ไม่แสวงหาผลกำไร) มีการรวบรวมอันดับการโจมตีระบบงาน/เว็บไซต์ และมีคำแนะนำในการดำเนินการป้องกัน เช่น การเรียนโปรแกรม การใช้เครื่องมือในการตรวจสอบการรักษาความมั่นคงปลอดภัย เทคโนโลยีที่ใช้ในการรักษาความปลอดภัย ซึ่งสามารถศึกษาและดาวน์โหลดเอกสารได้ที่ https://owasp.org/

คำแนะนำในการป้องกันและแก้ไข (Prevention)

สำหรับเว็บไซต์ที่พัฒนาด้วยภาษา PHP ควรกำหนดค่าในไฟล์ php.ini (เป็นไฟล์ที่ใช้กำหนดค่าของ PHP)เพื่อป้องกันไม่ให้สคริปต์ต่าง ๆ สามารถเรียกฟังก์ชันที่อาจก่อให้เกิดช่องโหว่จาก URL ภายนอกได้ ซึ่งมีค่า ที่ควรกำหนด ดังนี้

1. allow URL fopen off และ allow URL include off เพื่อป้องกันการโจมตีผ่านช่องโหว่ Remote file inclusion
2. ตรวจสอบ Input/Output ทุกครั้งที่มีการรับส่งข้อมูลบนเว็บไซต์ เพื่อป้องกันการรับ/ส่งค่า ที่เป็นอันตรายในการเข้าโจมตีเว็บไซต์ โดยแบ่งแยกประเภทและชนิดของข้อมูลที่รับ/ส่ง ให้ชัดเจน เพื่องายต่อการตรวจสอบ
3. ตรวจสอบ ประเภทของไฟล์ (File Extension) ที่ผ่านกระบวนการอัปโหลดไฟล์เข้ามา เพื่อป้องกันการอัปโหลดไฟล์อันตราย หรือไฟล์ที่จะก่อให้เกิดปัญหากับเครื่องแม่ข่ายของเว็บไซต์ และควรมีการกำหนดประเภทของไฟล์ที่อนุญาตให้สามารถอัปโหลดได้ (Whitelist)
4. ไม่เปิดสิทธิ์สำหรับการอ่าน-เขียนไฟล์หรือโค้ดของเว็บไซต์ให้กับผู้อื่น และหมั่นตรวจสอบวันที่อัปเดตไฟล์ (Date Modified) อยู่เสมอ
5. หากเป็น Third-party เช่น Joomla, WordPress หรือ Drupal ให้หมั่นตรวจเช็คข้อมูลจากเว็บไซต์ผู้พัฒนาอยู่เสมอ ๆ หากมีการประกาศรุ่นแพ็คเกจที่แก้ไขเรื่องความมั่นคงปลอดภัย ควรอัปเดตโดยทันที
6. ตรวจสอบว่ามีไฟล์อันตรายประเภท Remote shell ต่าง ๆ อยู่บนเครื่องแม่ข่ายที่ให้บริการเว็บไซต์หรือไม่ โดยให้ผู้ดูและระบบใช้โปรแกรมป้องกันไวรัสคอมพิวเตอร์ทั่วไป สแกนไปยังพื้นที่ของเว็บไซต์ที่ให้บริการ หรือส่วน plugins ของ CMS ที่ใช้งานอยู่ในปัจจุบัน
7. ควรสำรองข้อมูล (Backup) ของเว็บไซต์ไว้ที่อื่น นอกเหนือจากบนเครื่องแม่ข่ายที่ให้บริการอยู่

คำแนะนำในการป้องกันและแก้ไข (Web Defacement)

1. ตรวจสอบ และอัปเดตซอฟต์แวร์ ทั้งหมดที่ใช้กับเว็บไซต์ เช่น Webserver, CMS และ plugins ให้เป็นเวอร์ชันล่าสุดที่มีการแก้ไขช่องโหว่ความปลอดภัย โดยช่องโหว่ที่เกิดจากซอฟต์แวร์ที่ล้าสมัยอาจถูกใช้โดยผู้ไม่หวังดี เพื่อเข้าถึงเว็บไซต์ได้โดยไม่ได้รับอนุญาต
2. การตรวจสอบสิทธิ์การเข้าใช้งาน (Authentication) การใช้รหัสผ่านที่มีความปลอดภัย, การใช้งาน Multi-Factor Authentication (MFA) และการล็อคบัญชีเมื่อมีการพยายามเข้าใช้งานที่ไม่ได้รับอนุญาต เพื่อป้องกันการเข้าถึงบัญชีผู้ใช้โดยไม่ได้รับอนุญาต
3. การเรียนโค้ดที่ปลอดภัย เพื่อป้องกันช่องโหว่ทั่วไปของแอปพลิเคชันเว็บไซต์ เช่น SQL injection, Cross-site scripting (XSS), และ Cross-site request forgery (CSRF)

คำแนะนำในการป้องกันและแก้ไข (SQL Injection)

1. ทำ allow-list input เพื่อเน้นการบังคับให้ใช้รูปแบบข้อมูลที่อนุญาตเท่านั้น
2. ทำ escaping input ก่อนที่จะนำเอาค่านั้นไปประมวลผล
3. ทำ SQL statement / PDO เพื่อแบ่งระหว่าง command และ data (PHP ใช้ bindParam)
4. ตรวจสอบการตั้งค่าสิทธิ์การเข้าถึงไฟล์ให้มีความปลอดภัยมากยิ่งขึ้น

คำแนะนำในการป้องกันและแก้ไข (Directory Listing)

เว็บเซิร์ฟเวอร์ Apache:

1. เปิด.htaccess หรือ Apache config file (httpd.conf หรือ apache2.conf)
2. เพิ่มบรรทัดต่อไปนี้ภายในไฟล์ : Options -Indexes
3. บันทึกไฟล์และโหลดเว็บเซิร์ฟเวอร์ Apache

เว็บเซิร์ฟเวอร์ Nginx:

1. เปิดไฟล์ nginx.conf ค้นหาเซิร์ฟเวอร์สำหรับโดเมนหรือโฮสต์เสมือนที่ต้องการปิดการแสดงรายการไดเรกทอรี เพิ่มบรรทัดต่อไปนี้ภายในเซิร์ฟเวอร์ autoindex off
2. บันทึกไฟล์และโหลดเว็บเซิร์ฟเวอร์ Nginx

เว็บเซิร์ฟเวอร์ Microsoft IIS:

1. เปิด IS Manager และไปที่เว็บไซต์หรือไดเรกทอรีเสมือนที่ต้องการปิดการแสดงรายการไดเรกทอรี
2. คลิกที่ตัวเลือก Directory Browsing ในช่องแสดงคุณสมบัติ
3. คลิกที่ Disable ในช่องแสดงคำสั่งเพื่อปิดการแสดงรายการไดเรกทอรี