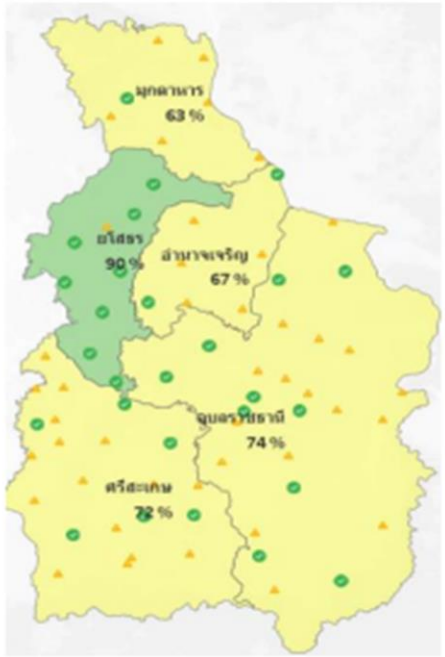
กลุ่มงานสุขภาพดิจิทัล

Cybersecurity



ศรีสะเกษ

ไม่มีความเสี่ยง รพ.สก

เสี่ยงต่ำ 2 แห่ง

เสี่ยงปานกลาง 19 แห่ง

เกณฑ์การประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์ และตัวชี้วัด ปี 2568 (Technology Cybersecurity Assessment Matrix : TAM)

เกณฑ์การประเมิน	ตัวชี้วัด			
	Q1	Q2	Q3	Q4
1. Backup 2. Antivirus Software 3. Access Control (Public และ Private) 4. Privileged Access Management (PAM)	โรงพยาบาลระดับ M1, S และ A ผ่านเกณฑ์ฯ ระดับสูง ร้อยละ 100	หน่วยงานผ่านเกณฑ์ฯ ระดับสูง ไม่น้อยกว่า ร้อยละ 50	- หน่วยงานผ่านเกณฑ์ฯ ระดับสูง ไม่น้อยกว่า ร้อยละ 80 - สสจ. และ สนข. ร้อยละ 100	หน่วยงานผ่านเกณฑ์ฯ ระดับสูง ร้อยละ 100
5. Business Continuity Plan (BCP) และ Disaster Recovery Plan (DRP) 6. OS Patching 7. Multi-Factor Authentication (2FA) 8. Web Application Firewall (WAF) 9. Log Management 10. Security Information & Event Management (SIEM) 11. Vulnerability Assessment (VA Scan)				
12. Software Update -> Optional 13. Penetration Testing -> Optional 14. Disaster Recovery site (DR) -> Optional				

หน่วยงานเป้าหมาย

- โรงพยาบาลศูนย์
- โรงพยาบาลทั่วไป
- โรงพยาบาลชุมชน เฉพาะที่เปิดให้บริการแล้ว
- สำนักงานสาธารณสุขจังหวัด (สสจ.)
- สำนักงานเขตสุขภาพที่ (สนข.) 1 - 12

การรายงาน

ทุกโรงพยาบาลส่งหลักฐานข้อมูลกลุ่มงานสุขภาพดิจิทัล ที่ e-mail yuparat.p@moph.mail.go.th ทุกวันอังคาร

หลักหลักฐานเชิงประจักษ์ที่หน่วยบริการต้องส่ง

1. Backup ตามระบบ 3-COPY 2- Media ที่แตกต่างกัน 1 - off site 1-offline 0-error
2. ภาพการติดตั้ง antivirus ใน server

3. ภาพการ config access control การจัดการสิทธิการเข้าถึงข้อมูล/ระบบ

4. ภาพการ config PAM

5. BCP , DRP เอกสารประกอบ DRP ต้องลงลึกขั้นตอนที่สามารถปฏิบัติได้จริง ต้องมากกว่า 1 หน้ากระดาษ

10. SIEM หน้าติดตั้ง ภาพหลักฐาน

11. VA Scan สรุปผลการทำ

หมายเหตุ ข้อ 11 อยู่ระหว่างประสาน สกมช. ให้สอนการทำ VA Scan

ข้อ 10 สสจ.จะจัดทำ SIEM จากโปรแกรม Wazuh เพื่อตรวจสอบช่องโหว่ในภาพรวมของจังหวัด ให้ รพ.ส่งข้อมูลเข้าระบบ โดย รพ. ต้องทำ SIEM เก็บข้อมูลจากเครื่อง Client ของ รพ.

THANK YOU