กรมอนามัย
กองแผนงาน

สรุปผลการประชุมเชิงปฏิบัติการขับเคลื่อนการดำเนินงาน ด้านความมั่นคงปลอดภัยสารสนเทศของกรมอนามัย

ระหว่างวันที่ 19 – 20 ธันวาคม 2567

ณ โรงแรมแกรนด์ริชมอนด์ จังหวัดนนทบุรี

จัดทำโดย

กลุ่มดิจิทัลส่งเสริมสุขภาพ

กองแผนงาน กรมอนามัย

สรุปการประชุมเชิงปฏิบัติการขับเคลื่อนการดำเนินงาน
ด้านความมั่นคงปลอดภัยสารสนเทศของกรมอนามัย
ระหว่างวันที่ 19 – 20 ธันวาคม 2567 ณ โรงแรมแกรนด์ริชมอนด์ จังหวัดนนทบุรี
****

ประธานเปิดการประชุม :

ดร.นายแพทย์ปองพล วรปาณิ รองอธิบดีกรมอนามัย

ผู้กล่าวรายงานการประชุม :

นายนุกูลกิจ พุกาธร ผู้อำนวยการกองแผนงาน

ผู้เข้าร่วมการประชุม : จำนวน 50 คน ประกอบด้วย

- ผู้บริหารกรมอนามัย
- บุคลากรกรมอนามัยทั้งส่วนกลางและส่วนภูมิภาค
- วิทยากร
- คณะทำงาน
- ผู้สังเกตการณ์

กองแผนงาน ได้จัดประชุมเชิงปฏิบัติการขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของกรมอนามัย ระหว่างวันที่ 19 – 20 ธันวาคม 2567 ณ โรงแรมแกรนด์ริชมอนด์ จังหวัดนนทบุรี เพื่อให้ผู้เข้าร่วมตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยไขเบอร์ สามารถป้องกันภัยคุกคามไซเบอร์ที่จะเกิดขึ้นในอนาคตได้อย่างทันท่วงที และมีแนวทางการดำเนินงานที่ถูกต้องเหมาะสม รวมทั้งมีความรู้และความเข้าใจด้านกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์สำหรับผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศของกรมอนามัย

กองแผนงาน ขอสรุปการจัดประชุมเชิงปฏิบัติการฯ ดังนี้

วันที่ 19 ธันวาคม 2567

1. ชี้แจงแนวทางการขับเคลื่อนด้านความมั่นคงปลอดภัยสารสนเทศของกรมอนามัย ประจำปีงบประมาณ พ.ศ. 2568”

โดย นายนุกูลกิจ พุกาธร ผู้อำนวยการกองแผนงาน

วัตถุประสงค์ : เพื่อชี้แจงแนวทางการขับเคลื่อนด้านความมั่นคงปลอดภัยสารสนเทศของกรมอนามัย

เนื้อหา/บทสรุป

กรมอนามัยเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญที่ต้องมีมาตรการ Cyber Security ตามมาตรฐานระดับประเทศ ปัจจุบันสถานการณ์ทางเทคโนโลยีมีภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างต่อเนื่อง จำเป็นต้องมีระบบป้องกันที่ทันสมัย ต้องยกระดับการเฝ้าระวังและปฏิบัติตามมาตรฐาน CTAM และ ISO/IEC 27001 การลงทุนด้าน Cyber Security และการพัฒนาบุคลากรเป็นสิ่งสำคัญ

1. กฎหมายและนโยบายด้าน Cyber Security ที่เกี่ยวข้อง

1.1 พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

- กำหนดให้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานหลักในการกำกับดูแล

- มีหน้าที่ป้องกันภัยคุกคามไซเบอร์ ร่วมมือกับภาครัฐและเอกชน และลดความเสี่ยงทางไซเบอร์

1.2 แผนปฏิบัติการด้าน Cyber Security ของประเทศไทย (2565-2570)

มี 4 ยุทธศาสตร์หลัก: Capacity – เพิ่มขีดความสามารถของประเทศ ,Partnership – บูรณาการความร่วมมือ , Resilience – ป้องกันและฟื้นฟูโครงสร้างพื้นฐาน และ Standard – ยกระดับมาตรฐาน

1.3 หน่วยงานที่เกี่ยวข้อง

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) แบ่งหน่วยงานที่ต้องปฏิบัติตามมาตรการ Cyber Security เป็น 4 กลุ่มหลัก: 1. Regulator – หน่วยงานกำกับดูแล 2. Government – หน่วยงานของรัฐ 3. CII (Critical Information Infrastructure) – หน่วยงานโครงสร้างพื้นฐานสำคัญ และ 4. CERT (Cybersecurity Emergency Response Team) – หน่วยงานรับมือภัยคุกคามไซเบอร์

กรมอนามัยอยู่ภายใต้หมวด CII เนื่องจากมีข้อมูลด้านสุขภาพที่สำคัญ หากถูกโจมตี อาจส่งผลกระทบต่อความปลอดภัยของประชาชนในวงกว้าง

2. นโยบาย Cyber Security ของกรมอนามัย

2.1 โครงสร้างการบริหารจัดการ Cyber Security

- CIO (Chief Information Officer) – บริหารระบบสารสนเทศ
- CISO (Chief Information Security Officer) – ควบคุมและตรวจสอบมาตรการความมั่นคงปลอดภัย
- CIRT (Cyber Incident Response Team) – ทีมรับมือภัยคุกคามไซเบอร์
- IT Staff – เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศในแต่ละหน่วยงาน

2.2 แนวทางการพัฒนาความมั่นคงปลอดภัยไซเบอร์ของกรมอนามัย

1) ยกระดับมาตรฐานและการเฝ้าระวังภัยคุกคาม
   - แต่งตั้งเจ้าหน้าที่ Cyber Security ประจำหน่วยงาน
   - ลงทุนในซอฟต์แวร์และเครื่องมือเฝ้าระวัง (SIEM, EDR, Firewall)
   - ปฏิบัติตามมาตรฐานสากล เช่น ISO/IEC 27001 และ 27799
2) พัฒนาศักยภาพบุคลากร
   - จัดอบรมและให้สอบใบรับรองด้าน Cyber Security
   - สนับสนุนค่าตอบแทนและค่าล่วงเวลา
3) เพิ่มขีดความสามารถของโครงสร้างพื้นฐาน
   - ลงทุนติดตั้งระบบ Next-Gen Firewall, IDS/IPS
   - ปรับปรุง Data Center และระบบเครือข่าย
   - พัฒนาระบบสำรองข้อมูล

3. สถานการณ์ภัยคุกคามทางไซเบอร์ที่พบในกรมอนามัย (ปี 2566-2567)

3.1 ประเภทของภัยคุกคามที่พบ

- Directory Listing – เปิดเผยรายการไฟล์บนเว็บไซต์
- Password Exposed – รหัสผ่านรั่วไหล
- PDPA Violation – การละเมิดข้อมูลส่วนบุคคล
- SQL Injection – การโจมตีฐานข้อมูล

- Ransomware – อยู่ระหว่างการตรวจสอบ

3.2 สถิติการโจมตี

- พบเหตุการณ์ด้านความมั่นคงปลอดภัยกว่า 2 ล้านครั้ง เฉลี่ยการโจมตี 10,000 ครั้ง/ปี โจมตีสำเร็จไปทั้งสิ้น 32 ครั้ง

ประเภทภัยคุกคาม	รายละเอียด	จำนวนครั้งที่พบ
Directory Listing	ระบบเปิดเผยรายการไฟล์และโฟลเดอร์ที่ไม่ควรถูกเข้าถึง	12 ครั้ง
Password Exposed	รหัสผ่านของผู้ใช้งานรั่วไหลบนอินเทอร์เน็ต	6 ครั้ง
PDPA Violation	มีการเผยแพร่ข้อมูลส่วนบุคคลโดยไม่ตั้งใจ	5 ครั้ง
SQL Injection	การโจมตีฐานข้อมูลเพื่อเข้าถึงหรือขโมยข้อมูล	6 ครั้ง
Web Skimming & Phishing	มีเว็บพนันออนไลน์ฝังอยู่ในหน้าเว็บไซต์ทางการของกรมอนามัย	2 ครั้ง
Ransomware	ถูกเข้ารหัสข้อมูลและเรียกค่าไถ่ (อยู่ระหว่างการตรวจสอบ)	1 ครั้ง

4. แผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

กรมอนามัยใช้ NIST Cybersecurity Framework ในการบริหารจัดการภัยคุกคาม

4.1 มาตรการเชิงรุก (Proactive Measures)

1) Risk Management:

- จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยี
- พัฒนาระบบความต่อเนื่องทางธุรกิจ (BCP)
- ซ้อมแผนรับมือเหตุการณ์ฉุกเฉิน

2) Security Investment:

- ติดตั้ง Next-Gen Firewall, IPS/IDS, XDR
- ลงทุนในระบบเฝ้าระวังภัยคุกคาม เช่น SEIM, EDR, DAST, SAST
- พัฒนาระบบสำรองข้อมูล

3) Governance & Compliance:

- ปฏิบัติตามมาตรฐาน CTAM และกฎหมาย PDPA
- ตรวจสอบและประเมินความเสี่ยงเป็นประจำ

4.2 มาตรการตอบสนอง (Incident Response Measures)

1) การตอบสนอง (Respond):

- ใช้ SIAM (Security Information and Management) ในการจัดการเหตุการณ์
- แจ้งเตือนและรายงานเหตุการณ์ตามข้อกำหนดของกฎหมาย
- ประสานงานกับ Health CERT และหน่วยงานกำกับดูแล

2) การฟื้นฟู (Recover):

- ใช้ BCP & Disaster Recovery Plan เพื่อกู้คืนระบบ
- กู้คืนข้อมูลจากระบบสำรอง
- ทบทวนและปรับปรุงมาตรการหลังเหตุการณ์

กรมอนามัยต้องเสริมสร้างมาตรการ Cyber Security อย่างเข้มงวด เนื่องจากมีภัยคุกคามเพิ่มขึ้นอย่างต่อเนื่อง การป้องกันที่ดีจะช่วยลดความเสี่ยงและปกป้องข้อมูลสำคัญของประชาชน

2. การบรรยาย เรื่อง "แนวทางการปฏิบัติและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Cyber Incident Response)"

วิทยากรโดย ว่าที่ร้อยตรี ภูวิช ชัยกรเริงเดช ผู้อำนวยการการฝ่ายสืบสวนและตรวจพิสูจน์หลักฐานทางไซเบอร์ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

วัตถุประสงค์ : เพื่อกำหนดแนวทางการปฏิบัติและตอบสนองต่อภัยคุกคามทางไซเบอร์ กรมอนามัย

เนื้อหา/บทสรุป

1. ความสำคัญของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงไซเบอร์เป็นกระบวนการสำคัญที่ช่วยให้หน่วยงานสามารถเข้าใจและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยมีเป้าหมายหลักดังนี้:

- ระบุเหตุการณ์ที่อาจเกิดขึ้น ("What Could Go Wrong") ซึ่งมักเป็นผลจากการโจมตีของผู้ไม่หวังดี
- กำหนดระดับของความเสี่ยง เพื่อช่วยให้สามารถจัดสรรทรัพยากรในการป้องกันได้อย่างเหมาะสม
- สร้างวัฒนธรรมหน่วยงานที่ตระหนักถึงความเสี่ยง โดยให้บุคลากรทุกระดับมีส่วนร่วมในการลดความเสี่ยง

2. กรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ หน่วยงานควรมีกระบวนการบริหารความเสี่ยงที่ชัดเจน ประกอบด้วย

- เอกสารแนวทางปฏิบัติ (Policy & Frameworks)
- เกณฑ์การประเมินความเสี่ยงและระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)
- ระบบเฝ้าระวังและติดตามความเสี่ยง (Risk Monitoring & Tracking)
- รวมความเสี่ยงไซเบอร์เป็นส่วนหนึ่งของการบริหารความเสี่ยงหน่วยงาน

3. การกำหนดบริบทและระดับของความเสี่ยง

3.1 การกำหนดบริบทของความเสี่ยง

- หน่วยงานต้องเข้าใจว่าความเสี่ยงไซเบอร์มีผลกระทบต่อการดำเนินงานอย่างไร
- มีการระบุผู้มีส่วนได้เสียที่เกี่ยวข้องทั้งภายในและภายนอก

3.2 การกำหนดความเสี่ยง (Define Risk)

ระดับของความเสี่ยงพิจารณาจาก โอกาสเกิด (Likelihood) และ ผลกระทบ (Impact)

ตามสมการ : Risk = Function (Likelihood, Impact)

3.3 ปัจจัยที่ส่งผลต่อความเสี่ยง

1. เหตุการณ์ภัยคุกคาม (Threat Event) - การกระทำของผู้โจมตีที่อาจส่งผลเสียหายต่อระบบ
2. ช่องโหว่ (Vulnerability) - จุดอ่อนของระบบที่อาจถูกโจมตีได้
3. โอกาสเกิด (Likelihood) - ความเป็นไปได้ที่ภัยคุกคามจะเกิดขึ้น
4. ผลกระทบ (Impact) - ความเสียหายที่อาจเกิดขึ้นหากถูกโจมตีสำเร็จ

3.4 การกำหนดระดับความเสี่ยงที่ยอมรับได้

- สูง (High) ⟶ ต้องแก้ไขทันที เพราะอาจทำให้กิจกรรมต้องหยุดลง
- กลาง (Medium) ⟶ ต้องลดความเสี่ยงภายใน 3-6 เดือน
- ต่ำ (Low) ⟶ อาจยอมรับได้แต่ต้องเฝ้าระวัง

4. การประเมินความเสี่ยงทางไซเบอร์ กระบวนการประเมินความเสี่ยงแบ่งเป็น 3 ขั้นตอน

4.1 การระบุความเสี่ยง (Risk Identification)

- ระบุทรัพย์สินสำคัญ (Identify Assets) เช่น ฐานข้อมูล, ระบบเครือข่าย
- การสร้างแบบจำลองภัยคุกคาม (Threat Modelling)
  - กำหนดขอบเขตของระบบ
  - ระบุภัยคุกคามที่เป็นไปได้
  - สร้างแบบจำลองการโจมตี
- สร้างสถานการณ์ความเสี่ยง (Risk Scenario Construction)
  - ระบุสินทรัพย์ ⟶ ระบุภัยคุกคาม ⟶ ระบุช่องโหว่ ⟶ วิเคราะห์ผลกระทบ

ตัวอย่างสถานการณ์ความเสี่ยง

- การโจมตี SQL Injection เพื่อล้วงข้อมูลเวชระเบียนผู้ป่วย
- พนักงานถูกหลอกให้ทำธุรกรรมผิดพลาด
- ผู้บุกรุกเข้าถึงระบบ SCADA และปิดระบบน้ำประปา
- อีเมลฟิชชิ่ง (Phishing mail) ที่ขโมยข้อมูลบัญชีผู้ใช้

4.2 การวิเคราะห์ความเสี่ยง (Risk Analysis)

- กำหนดโอกาสเกิด (Determine Likelihood)
- กำหนดผลกระทบ (Determine Impact)

4.3 การประเมินความเสี่ยง (Risk Evaluation)

- จัดลำดับความสำคัญของความเสี่ยง
- บันทึกลงทะเบียนความเสี่ยงเพื่อใช้ติดตามและปรับปรุงมาตรการ

5. การตอบสนองต่อความเสี่ยง (Risk Response) หน่วยงานสามารถเลือกแนวทางจัดการความเสี่ยงได้ดังนี้

- ยอมรับ (Accept) ⟶ หากความเสี่ยงต่ำและผลกระทบจำกัด
- หลีกเลี่ยง (Avoid) ⟶ เปลี่ยนแปลงกระบวนการทำงานเพื่อลดความเสี่ยง
- โอนย้าย (Transfer) ⟶ ใช้ประกันภัยหรือให้บุคคลภายนอกรับผิดชอบ
- ลดความเสี่ยง (Mitigate) ⟶ นำมาตรการป้องกันมาใช้ เช่น การเข้ารหัสข้อมูล

6. แผนรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) แผนการรับมือแบ่งออกเป็น 4 ขั้นตอน

6.1 การเตรียมการ (Preparation)

- จัดตั้ง ทีมรับมือเหตุการณ์ไซเบอร์ (CIRT - Cyber Incident Response Team)
- กำหนดโครงสร้างการรายงานเหตุการณ์
- สร้างแผนสำรองและมาตรการตอบสนอง

6.2 การตรวจจับและวิเคราะห์ (Detection & Analysis)

- ใช้ระบบเฝ้าระวังภัยคุกคาม (SIEM, IDS/IPS)
- วิเคราะห์รูปแบบการโจมตีเพื่อกำหนดมาตรการตอบโต้

6.3 การระงับและกู้คืนระบบ (Containment, Eradication & Recovery)

- จำกัดขอบเขตของการโจมตีเพื่อลดความเสียหาย
- กู้คืนระบบจากข้อมูลสำรอง
- เก็บหลักฐานเพื่อสืบสวนหาต้นตอของการโจมตี

6.4 การทบทวนหลังเหตุการณ์ (Post-Incident Activity)

- ประเมินผลการตอบสนองและหาแนวทางปรับปรุง
- ปรับมาตรการความปลอดภัยเพื่อป้องกันเหตุการณ์ในอนาคต

7. แหล่งเรียนรู้และพัฒนาทักษะไซเบอร์

- National Cyber Security Agency (NCSA) มีหลักสูตรอบรมและ Certification ฟรี
- เปิดให้บุคลากรทุกระดับสามารถ Upskill & Reskill ด้านไซเบอร์

<u>จากการบรรยายครั้งนี้</u> เน้นความสำคัญของการประเมินความเสี่ยงทางไซเบอร์และการจัดทำแผนรับมือเหตุการณ์ไซเบอร์ที่มีประสิทธิภาพ โดยให้ความสำคัญกับ

- ✓ การวิเคราะห์ความเสี่ยง เพื่อระบุและจัดลำดับความสำคัญของภัยคุกคาม
- ✓ การตอบสนองต่อความเสี่ยง โดยใช้มาตรการป้องกันและลดความเสียหาย
- ✓ การจัดตั้งทีมรับมือเหตุการณ์ไซเบอร์ (CIRT) เพื่อรับมือกับภัยคุกคามในอนาคต

หน่วยงานควรนำแนวทางเหล่านี้ไปปรับใช้เพื่อเพิ่มความปลอดภัยของข้อมูลและระบบสารสนเทศ

3. การบรรยายเรื่อง "การตรวจสอบช่องโหว่เบื้องต้นด้วยโปรแกรม Nessus เพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย" และการฝึกปฏิบัติ เรื่อง "การวิเคราะห์และประเมินจุดอ่อน (Vulnerability Assessment) ด้วยโปรแกรม Nessus"

วิทยากรโดย นายพงษ์ศักดิ์ ทองประหยัด System Engineer
นางสาวศรัญญา เจริญผล Product Manager
บริษัท นิช-เอส โซลูชั่น จำกัด

วัตถุประสงค์ : เพื่อสอนการใช้งานการตรวจสอบช่องโหว่เบื้องต้นด้วยโปรแกรม Nessus

เนื้อหา/บทสรุป

1. ความหมายของช่องโหว่ (Vulnerability)

ช่องโหว่คือ จุดอ่อนของระบบ ที่อาจถูกใช้โดยผู้โจมตีเพื่อลดทอนการรักษาความมั่นคงปลอดภัยของข้อมูล โดยมีองค์ประกอบหลัก 3 ส่วน ได้แก่

- ข้อตำหนิของระบบ (Weakness) ที่สามารถถูกโจมตี
- ผู้โจมตีที่สามารถเข้าถึงช่องโหว่นั้น
- เครื่องมือหรือเทคนิคที่ใช้ในการโจมตี

ช่องโหว่เป็นส่วนหนึ่งของ พื้นหน้าของการโจมตี (Attack Surface) ซึ่งหมายถึงจุดที่ระบบเปิดโอกาสให้ถูกโจมตีได้

2. การจัดการช่องโหว่ (Vulnerability Management)

การจัดการช่องโหว่เป็น กระบวนการเชิงวัฏจักร ที่เกี่ยวข้องกับการ

- ระบุ (Identify)
- จำแนก (Categorize)
- เยียวยา (Remediate)
- บรรเทาผลกระทบ (Mitigate)

โดยช่องโหว่บางประเภทอาจไม่ก่อให้เกิดความเสี่ยงเสมอไป เช่น ช่องโหว่ที่กระทบกับสินทรัพย์ที่ไม่มีมูลค่า

3. องค์ประกอบของการโจมตีทางไซเบอร์

1. เติบโตขึ้น – จำนวนช่องโหว่เพิ่มขึ้นอย่างต่อเนื่อง
2. ยืดหยุ่นมากขึ้น – วิธีการโจมตีมีความซับซ้อนและพัฒนาอย่างรวดเร็ว
3. แพร่กระจายในวงกว้างมากขึ้น – มีหลายช่องทางที่สามารถใช้โจมตีได้ เช่น เว็บไซต์หรือเซิร์ฟเวอร์

4. ช่องทางที่อาจถูกโจมตี ดังนี้

1. อุปกรณ์ปลายทาง (Endpoint Devices) – เช่น โน้ตบุ๊กหรือมือถือ
2. โดเมนหน่วยงาน (Domain Enumeration) – ค้นหาโดเมนที่เกี่ยวข้องเพื่อล้วงข้อมูล
3. Web Application / Internal Web – เว็บไซต์และระบบภายในหน่วยงาน
4. Public Cloud – บริการคลาวด์ที่อาจมีการตั้งค่าไม่ปลอดภัย
5. OT/IoT (Operational Technology & Internet of Things) – อุปกรณ์อัจฉริยะ เช่น เครื่องจักรในโรงงาน, เครื่องมือแพทย์
6. Identity Management System – ระบบที่เก็บข้อมูลสำคัญของหน่วยงาน

5. ระบบ Nessus และการใช้งาน

Nessus เป็นระบบตรวจสอบช่องโหว่และการตั้งค่าความปลอดภัยที่ได้รับการยอมรับในระดับสากล ซึ่งช่วยให้สามารถ ตรวจสอบอุปกรณ์ในเครือข่าย วิเคราะห์การตั้งค่าความปลอดภัย ค้นหา Malware และช่องโหว่โดยอัตโนมัติ ปรับแต่งการสแกนและรายงานผล

ข้อดีของ Nessus

- มีทีมวิเคราะห์ข้อมูลจาก Dark Web และ Social Media เพื่อเก็บข้อมูลความเสี่ยง
- รองรับการใช้งานในหลายอุตสาหกรรม

6. ขั้นตอนการตรวจสอบช่องโหว่ของ Nessus (5 ขั้นตอน)

1. Discovery – ตรวจสอบอุปกรณ์ที่ออนไลน์
2. Assessment – สแกนหาช่องโหว่
    - สแกนแบบระบุ User/Pass (Provincial)
    - สแกนแบบไม่ใช้รหัสผ่าน (External Scan)
3. Prioritize – จัดลำดับความรุนแรงของช่องโหว่เป็น 5 ระดับ
    - Critical, High, Medium, Low และ Info
4. Fix – แนะนำวิธีแก้ไข แต่ระบบไม่สามารถปิดช่องโหว่เองได้
5. Measure – สแกนซ้ำเพื่อตรวจสอบว่าช่องโหว่ถูกปิดแล้วหรือไม่

7. การวิเคราะห์และจัดลำดับการแก้ไข

- VPR (Vulnerability Priority Rating): ปรับคะแนนความรุนแรงของช่องโหว่ตามเหตุการณ์และความจำเป็น
- ACR (Asset Criticality Rating): จัดลำดับความสำคัญของช่องโหว่ที่ต้องแก้ไข

8. ฟีเจอร์เด่นของ Nessus

- สรุป 10 อันดับช่องโหว่ที่สำคัญที่สุด
- สามารถสร้างและปรับแต่งรายงานได้หลายรูปแบบ (HTML, CSV, XML)
- Live Results – วิเคราะห์ช่องโหว่แบบอัตโนมัติและแสดงผลทันที
- จัดกลุ่มช่องโหว่ที่คล้ายกัน เพื่อให้แก้ไขได้ง่ายขึ้น

สรุปการใช้งานโปรแกรม Nessus เป็นเครื่องมือที่ช่วยหน่วยงาน วิเคราะห์และจัดการช่องโหว่ได้อย่างมีประสิทธิภาพ ผ่านกระบวนการตรวจสอบ 5 ขั้นตอน และสามารถปรับแต่งการจัดลำดับความสำคัญของช่องโหว่ได้ ซึ่งช่วยให้สามารถปิดจุดอ่อนของระบบได้อย่างรวดเร็วและแม่นยำ

วันที่ 20 ธันวาคม 2567

5. การอภิปราย เรื่อง กรมอนามัยกับแนวทางป้องกันการละเมิดข้อมูลส่วนบุคคล (PDPA)

ผู้ร่วมอภิปราย

1) นายสมเกียรติ ปฏิรพ หัวหน้ากลุ่มดิจิทัลส่งเสริมสุขภาพ กองแผนงาน

2) นายนันทวัฒน์ จองคำ นักวิชาการคอมพิวเตอร์ปฏิบัติการ กองการเจ้าหน้าที่

3) นางสาวลดาวัลย์ จิตขาว นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักอนามัยการเจริญพันธุ์

4) นายจิระเดช นงษ์รัก นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ 5 ราชบุรี

ผู้ดำเนินการอภิปราย นายสุชาญ กิจลือเลิศ กองแผนงาน

วัตถุประสงค์ : เพื่อแลกเปลี่ยนเรียนรู้ ประสบการณ์ การดำเนินงานความปลอดภัยทางไซเบอร์ และการละเมิดข้อมูลส่วนบุคคล

เนื้อหา/บทสรุป

1. ประเด็นด้านความปลอดภัยของข้อมูลและการป้องกันการโจมตีทางไซเบอร์

- มีการโจมตีทางไซเบอร์มากกว่า 10,000 ครั้งต่อปี กรมอนามัยจำเป็นต้องเสริมมาตรการป้องกันข้อมูลส่วนบุคคล
- มีเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหล รวมถึงการละเมิดข้อมูลบน "ถุงกล้วยแขก" หน่วยงานที่เกี่ยวข้องต้องดำเนินการชี้แจงที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)
- กำหนดให้มี **Data Processor และ Data Controller** ดูแลข้อมูล และปรับแนวทางการทำลายข้อมูลอย่างปลอดภัย
- กองแผนงานออกแนวทางการจัดเก็บและทำลายเอกสาร ทั้งแบบกระดาษและอิเล็กทรอนิกส์

2. การโจมตีระบบ HR และแนวทางแก้ไข

- ระบบ HR ของกรมอนามัยถูกโจมตีด้วย **SQL Injection** ส่งผลให้ต้องรีเซ็ตรหัสผ่าน และเสริมมาตรการความปลอดภัย
- มีแนวทางเพิ่มฟังก์ชันการกด **Consent Form** เพื่อให้ผู้ใช้งานยืนยันการเข้าถึงข้อมูล
- มีการใช้ **NextGen Firewall, Honeypot, GMS และ SIEM Analyst** เพื่อวิเคราะห์ข้อมูลการโจมตี
- ระบบ HR จะได้รับการบำรุงรักษาและปรับปรุงความปลอดภัยตามงบประมาณปี 2569

3. กรณีข้อมูลส่วนบุคคลรั่วไหลบน Dark Web

- สำนักสุขาภิบาลอาหารและน้ำพบข้อมูลหลุดไปขายบน Dark Web และดำเนินการร่วมกับผู้เชี่ยวชาญจาก สป. มาตรวจสอบ และแจ้ง สกมช. ทำ VA Scan พร้อมแจ้งความกับตำรวจไซเบอร์
- ระบบเฝ้าระวังการแท้งประเทศไทย ถูกโจมตีและพบว่ามีข้อมูลรั่วไหล เนื่องจากระบบเก่าและขาดการบำรุงรักษา ให้ปิดระบบชั่วคราว และใช้ Google Form ในการเก็บข้อมูลแทน
- ให้แยกข้อมูลที่อ่อนไหวออกจากข้อมูลทั่วไป และปรับระบบให้ไม่แสดงข้อมูลส่วนบุคคล

4. การรับมือเหตุการณ์ด้านความปลอดภัยไซเบอร์ในศูนย์อนามัยต่าง ๆ

- **ศูนย์อนามัยที่ 5** ถูกโจมตี ทำให้ข้อมูลผู้ใช้ 135 รายหลุดไป มีความพยายามล็อกอินกว่า 40,000 ครั้ง แนวทางแก้ไข ปรับ **Password Policy**, เพิ่ม **CAPTCHA**, และตรวจสอบ Log
- **ศูนย์อนามัยที่ 2** พบการโจมตีแบบ **SQL Injection** และแก้ไขโดยใช้ **Encryption** สำหรับรหัสผ่าน

- **ศูนย์อนามัยที่ 10** ถูกโจมตีด้วย **Ransomware** แต่สามารถกู้คืนข้อมูลจาก **Backup** ได้

5. แนวทางปรับปรุงนโยบายและมาตรการรักษาความปลอดภัยข้อมูล

- การจัดทำ **Privacy Notice** สำหรับระบบ HR
- ศูนย์อนามัยต้องกำหนด **Data Processor และ Data Controller** อย่างชัดเจน
- นโยบายเกี่ยวกับ Consent Form: หากมีกฎหมายรองรับ ไม่จำเป็นต้องใช้
- การใช้ระบบ Cloud ของกรมอนามัย ต้องผ่านการคัดเลือกตามเกณฑ์ที่กำหนด

6. การดำเนินงานในอนาคต

- กองแผนงานจะช่วยตรวจสอบและเสริมมาตรการรักษาความปลอดภัย
- ศูนย์อนามัยต่าง ๆ ต้องดำเนินการปรับปรุงระบบ **DCP และ BRP** (Disaster Recovery Plan) เอง หากเร่งด่วนให้ใช้งบประมาณของตัวเอง
- การเชื่อมต่อระบบดิจิทัลของกรมอนามัยในอนาคต จะรวมกับ **Health Book** เท่านั้น

ข้อสรุปสำคัญ: ต้องเร่งเสริมมาตรการรักษาความปลอดภัยข้อมูล ปรับปรุงระบบที่ล้าสมัย และเพิ่มการรับมือภัยคุกคามทางไซเบอร์ในทุกระดับ ดังนี้

1. หน่วยงานต้อง **เพิ่มมาตรการความปลอดภัยทางไซเบอร์**
2. ให้ **ทุกหน่วยงานส่ง Log มายังกองแผนงาน** เพื่อตรวจสอบความผิดปกติ
3. การพัฒนาระบบใหม่ต้องผ่าน **คณะกรรมการคลัสเตอร์ กลุ่มที่ 5 กลุ่มพัฒนาระบบดิจิทัลฯ**
4. ให้ความสำคัญกับ **การป้องกันข้อมูลรั่วไหลและการรักษาความปลอดภัยของระบบ**

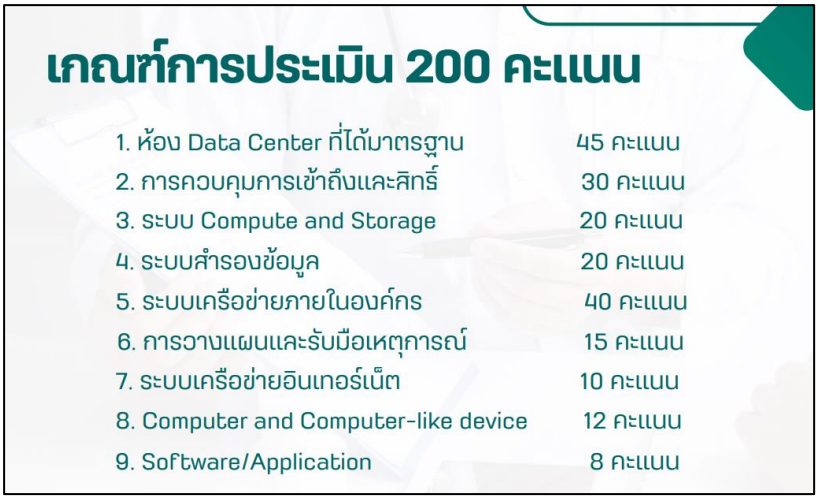
6. ชี้แจงเกณฑ์การประเมินระดับความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐาน (CTAM: Cybersecurity Technical Assessment Matrix)

โดย นายสุชาญ กิจลือเลิศ กองแผนงาน

วัตถุประสงค์ : เพื่อเป็นแนวทางในการประเมินระดับความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานของกรมอนามัย

เนื้อหา/บทสรุป

สรุปประเด็นยกระดับความมั่นคงปลอดภัยทางไซเบอร์สำหรับหน่วยบริการสุขภาพ กรมอนามัย โดยอ้างอิงจากแนวทางการประเมิน CTAM และโรงพยาบาลอัจฉริยะ ซึ่งแบ่งการประเมินเป็น 9 หมวดหลัก รวมคะแนนทั้งหมด 200 คะแนน ดังนี้:



สรุปแนวทางการดำเนินงาน เพื่อจัดทำแผนพัฒนางานด้าน Cyber Security ของกรมอนามัย

- ปรับปรุงโครงสร้างพื้นฐาน ⟶ อัปเกรด Storage, Network และ Power Management
- เพิ่มความปลอดภัยทางไซเบอร์ ⟶ ใช้ Zero Trust, AI-driven Security และทำ Pen Test
- ปรับปรุงการบริหารจัดการระบบ ⟶ ใช้ Automation, AI Monitoring และ SIEM
- พัฒนาบุคลากร ⟶ อบรมด้าน Security, Compliance และ Data Governance
- นำเทคโนโลยีใหม่มาใช้ ⟶ AI, Cloud, Blockchain และ Predictive Analytics

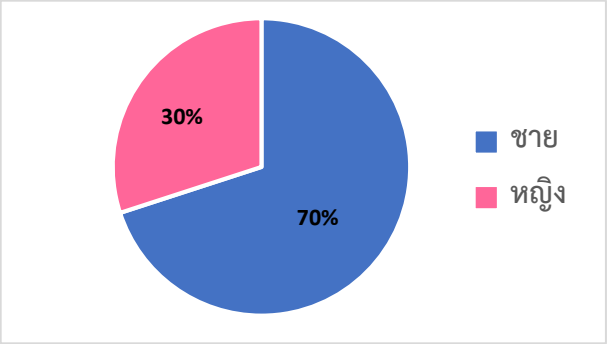
การดำเนินงานต่อไป

1. เตรียมจัดทำแผนและแนวทางชี้แจงเกณฑ์การประเมินระดับความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานของกรมอนามัย เพื่อเตรียมความพร้อมด้าน Cyber Security หน่วยงานสังกัดกรมอนามัยนำไปใช้ตามเป้าหมายที่กำหนด
2. จัดทำข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมอนามัย

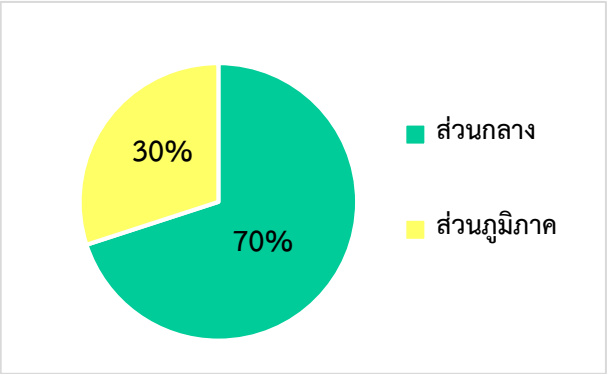
สรุปแบบประเมินความพึงพอใจในการจัดการประชุมเชิงปฏิบัติการ
ขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ ของกรมอนามัย

1. ข้อมูลทั่วไป

1.1 เพศ

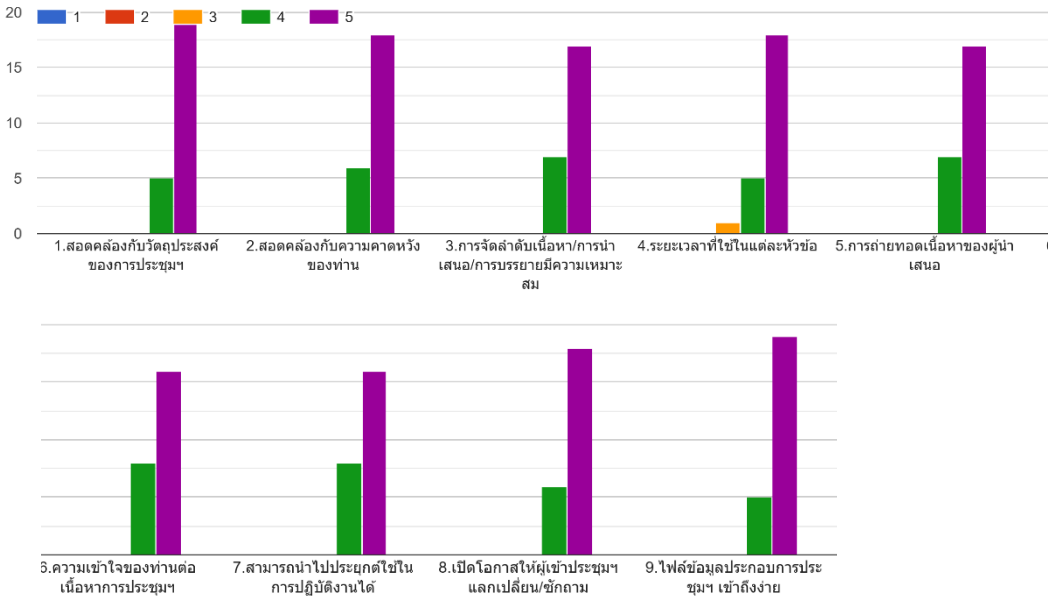


1.2 หน่วยงาน



2. ระดับความพึงพอใจต่อการประชุมฯ

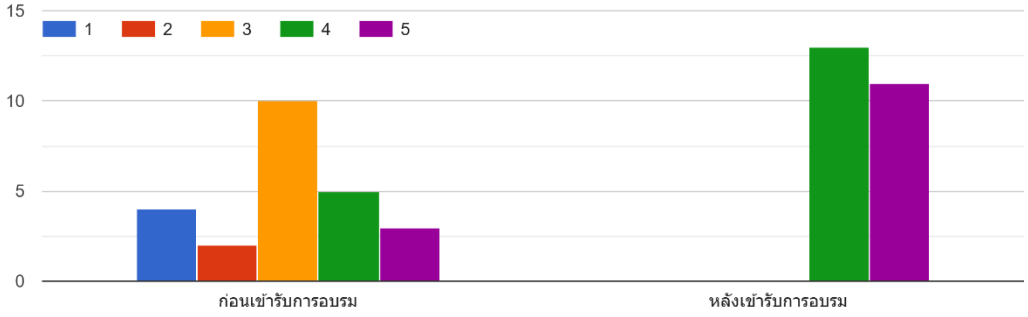
2.1 เนื้อหาการประชุมฯ



2.2 บุคลากรมีความรู้เพิ่มขึ้น หรือมากกว่าก่อนเข้ารับการประชุม

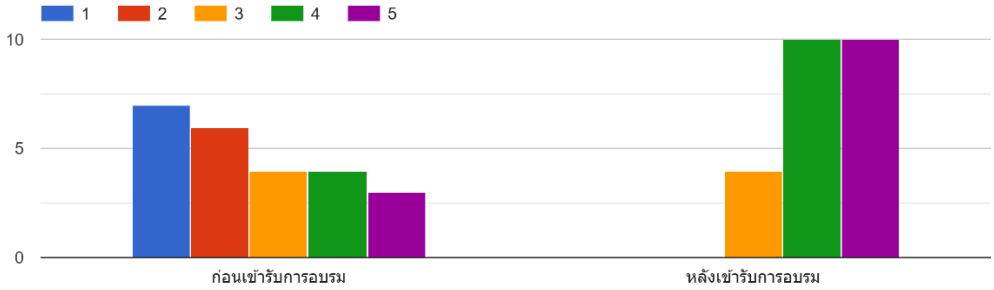
2.2.1 หัวข้อ "แนวทางการปฏิบัติและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Cyber Incident Response)"

โดย ว่าที่ร้อยตรี ภูวิช ชัยกรเริงเดช



2.2.2 หัวข้อ "การตรวจสอบช่องโหว่เบื้องต้นด้วยโปรแกรม Nessus เพื่อการรักษาความมั่นคง ปลอดภัยทางไซเบอร์ กรมอนามัย"

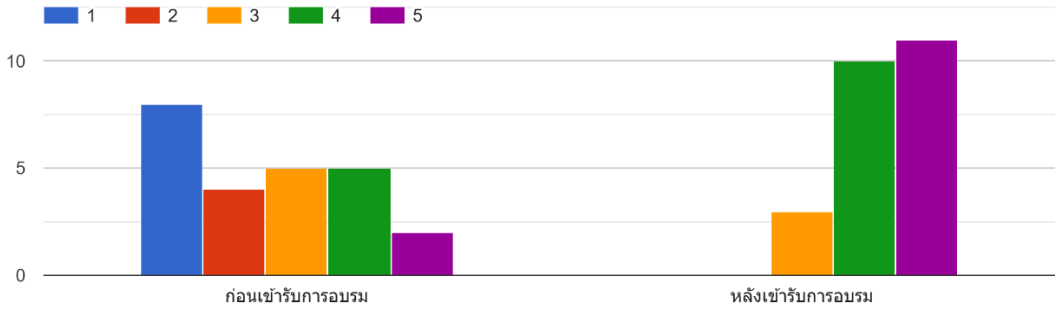
โดย คุณพงษ์ศักดิ์ ทองประหยัด ตำแหน่ง System Engineer บริษัท นิช-เอส โซลูชั่น จำกัด



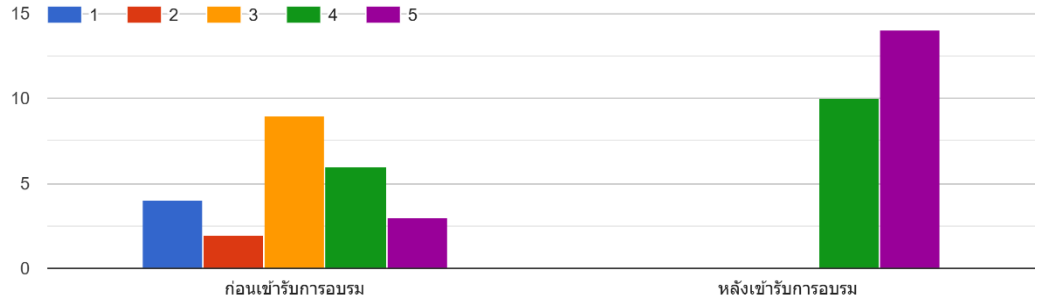
2.2.3 หัวข้อ "การฝึกปฏิบัติ เรื่อง “การวิเคราะห์และประเมินจุดอ่อน (Vulnerability Assessment) ด้วยโปรแกรม Nessus"

โดย คุณพงษ์ศักดิ์ ทองประหยัด ตำแหน่ง System Engineer

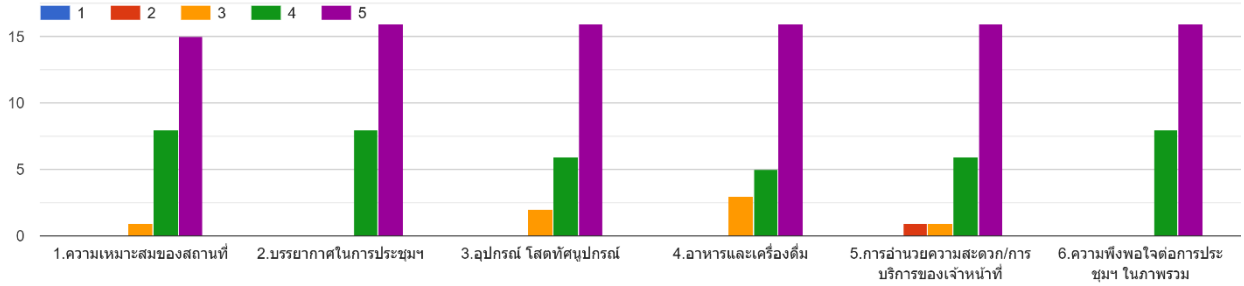
และ คุณศรัญญา เจริญผล ตำแหน่ง Product Manager บริษัท นิช-เอส โซลูชั่น จำกัด



2.2.4 หัวข้อ การอภิปราย "กรมอนามัยกับแนวทางป้องกันการละเมิดข้อมูลส่วนบุคคล (PDPA)"



2.3 สถานที่จัดประชุม/อาหาร/อื่นๆ



ภาคผนวก

- ภาพการประชุม
- เอกสารการประชุม

ภาพประกอบการประชุมเชิงปฏิบัติการ

ขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ ของกรมอนามัย

PUSH

กรมอนามัย
Department Of Health
ประชุมเชิงปฏิบัติการ
การขับเคลื่อนการดำเนินงาน
ด้านความมั่นคงปลอดภัยสารสนเทศ
ของกรมอนามัย
วันที่ 19 - 20 ธันวาคม 2567
ณ ห้องประชุม Peridot ชั้น 3 ตึก East wing
โรงแรมเทรนดี้รีสอร์ท จังหวัดนนทบุรี

1,827

tenable

tenable
network security
Transform
your Security with
Tenable
Creators of Nessus & Leaders in
Continuous Monitoring
tenable.com

กรมอนามัยกับแนวทางป้องกัน
การละเมิดข้อมูลส่วนบุคคล
(PDPA : Personal Data Protection Act)

กรมอนามัย
Department Of Health
ประชุมเชิงปฏิบัติการ
การขับเคลื่อนการดำเนินงาน
ของกรมอนามัย
วันที่ 19 - 20 ธันวาคม 2567
ห้องประชุม Peridot ชั้น 3 ตึก East wing
โรงแรมดิรัมดอนด์ จังหวัดนนทบุรี

แสกน QR Code

เอกสารประกอบการประชุม