รายงานสรุปผลการฝึกซ้อมแผนเผชิญเหตุและรับมือภัยคุกคามทางไซเบอร์
โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต ประจำปีงบประมาณ ๒๕๖๙

๑. บทนำและวัตถุประสงค์

ด้วยสถานการณ์ปัจจุบัน ภัยคุกคามทางไซเบอร์โดยเฉพาะมัลแวร์เรียกค่าไถ่ (Ransomware) ได้สร้างความเสียหายต่อระบบโครงสร้างพื้นฐานของหน่วยงานสาธารณสุขอย่างต่อเนื่อง เพื่อให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และมาตรฐานระบบเทคโนโลยีสารสนเทศโรงพยาบาล ศูนย์เทคโนโลยีสารสนเทศ โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต จึงได้จัดการฝึกซ้อมแผนเผชิญเหตุ (Incident Response Plan - IRP) ประจำปี ๒๕๖๙ รูปแบบสถานการณ์จำลองบนโต๊ะ (Tabletop Exercise) โดยมีวัตถุประสงค์ดังนี้

๑. เพื่อทดสอบความเข้าใจในบทบาทหน้าที่ของทีมรับมือเหตุฉุกเฉิน (Incident Response Team)

๒. เพื่อประเมินประสิทธิภาพของขั้นตอนการปฏิบัติงานมาตรฐาน (SOP) ในการกักกัน (Containment) และกู้คืนระบบ (Recovery)

๓. เพื่อทดสอบความพร้อมของระบบสำรองข้อมูล Proxmox Backup Server (PBS) และประสิทธิภาพของอุปกรณ์รักษาความปลอดภัยเครือข่าย (Firewall FortiGate)

๔. เพื่อค้นหาช่องโหว่ในกระบวนการปฏิบัติงาน นำไปสู่การปรับปรุงและอุดช่องโหว่ (Continuous Improvement)

๒. ข้อมูลทั่วไปและโครงสร้างการฝึกซ้อม (Exercise Overview)

๒.๑. รูปแบบการฝึกซ้อม การจำลองสถานการณ์และระดมสมองแก้ไขปัญหา (Tabletop Simulation)

๒.๒. วันที่ดำเนินการฝึกซ้อม วันพฤหัสบดีที่ ๕ มีนาคม ๒๕๖๙ เวลา ๑๓.๐๐ - ๑๖.๓๐ น.

๒.๓. สถานที่ ห้องประชุมศูนย์เทคโนโลยีสารสนเทศ โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต

๒.๔.สถานการณ์จำลองหลัก (Main Scenario) การโจมตีด้วยมัลแวร์เรียกค่าไถ่ (Ransomware) ผ่านช่องทาง Phishing Email บริเวณตึกผู้ป่วยนอก (OPD) และความพยายามในการขยายวงการโจมตี (Lateral Movement) เข้าสู่ระบบฐานข้อมูล HOSxP

๓. รายชื่อคณะทำงานและผู้เข้าร่วมการฝึกซ้อม (Exercise Attendees)

ลำดับ	ชื่อ - นามสกุล	บทบาทในการฝึกซ้อมตามแผน IRP
๑	นางศิริกัญญา ถาบุตร	ผู้บัญชาการเหตุการณ์ (Incident Commander)
๒	นายวชิรวิทย์ อุดมฉวี	ผู้ปฏิบัติการทางเทคนิค / Network & Server Admin
๓	นายพงษ์ดนัย วรสาร	ผู้ปฏิบัติการทางเทคนิค / Database Admin
๔	น.ส.ขวัญฤดี นามนนท์	ผู้ช่วยประสานงานและบันทึกเหตุการณ์ (Log Keeper)
๕	น.ส.พัชราภรณ์ แสงหาญ	ผู้ปฏิบัติการทางเทคนิค / IT Support (ผู้รับแจ้งเหตุ)
๖	น.ส.วรรณนิดา นามแสง	ผู้ปฏิบัติการทางเทคนิค / IT Support
๗	นายอภิวัฒน์ อินธิกาย	ผู้ปฏิบัติการทางเทคนิค / IT Support
๘	นายชนุดม อาษา	ผู้ปฏิบัติการทางเทคนิค / IT Support

๔. บันทึกลำดับเหตุการณ์จำลองและการตอบสนอง (Timeline & Response Log) การฝึกซ้อมได้ดำเนินตามกรอบมาตรฐานการรับมือเหตุฉุกเฉิน (Incident Response Life Cycle) ดังนี้

๔.๑. การตรวจพบและการวิเคราะห์ (Detection & Analysis)

- ๑๓.๐๐ น. น.ส.พัชราภรณ์ แสงหาญ (เวร On Call) รับแจ้งเหตุฉุกเฉินจากพยาบาลจุดซักประวัติ ตึก OPD ว่าหน้าจอคอมพิวเตอร์เปลี่ยนเป็นข้อความเรียกค่าไถ่ และไฟล์เอกสารในเครื่องถูกเปลี่ยนนามสกุล ไม่สามารถเปิดใช้งานระบบ HOSxP ได้
- ๑๓.๐๕ น. ทีม IT Support รีโมทเข้าตรวจสอบและยืนยันสถานการณ์ว่าเป็นการโจมตีของ Ransomware น.ส.พัชราภรณ์ แสงหาญ ดำเนินการยกระดับเหตุการณ์ (Escalation) รายงานต่อ นางศิริกัญญา ถาบุตร (Incident Commander) ทันที

๔.๒. การจำกัดความเสียหาย (Containment)

- ๑๓.๑๐ น. นางศิริกัญญา ถาบุตร ประกาศใช้แผนเผชิญเหตุระดับสูง (Critical) สั่งการให้ทีมงานลงพื้นที่และตัดระบบที่เกี่ยวข้อง
- ๑๓.๑๕ น. นายอภิวัฒน์ อินธิกาย และ นายชนุดม อาษา ถึงพื้นที่จุดเกิดเหตุ ดำเนินการสั่ง "ถอดสาย LAN" คอมพิวเตอร์เป้าหมายจำนวน ๓ เครื่องทันที พร้อมกำชับบุคลากรห้าม Shut down เครื่องเพื่อรักษาหลักฐานทางดิจิทัล (Digital Forensics) ในหน่วยความจำ
- ๑๓.๒๐ น. นายวชิรวิทย์ อุดมฉวี ตรวจสอบการจราจรบนเครือข่าย และเข้าตั้งค่า Firewall FortiGate เพื่อเปิดใช้กฎฉุกเฉิน (Emergency Rule) ทำการ Block Traffic จากวง LAN ของตึก OPD ทั้งหมด ไม่ให้สามารถเชื่อมต่อกับวง Server ของ Proxmox Cluster และ Ceph Storage เพื่อป้องกันการแพร่กระจาย

๔.๓. การกำจัดภัยคุกคาม (Eradication)

- ๑๓.๔๕ น. นายวชิรวิทย์ อุดมฉวี และ นายพงษ์ดนัย วรสาร ตรวจสอบ Log บนสวิตช์เครือข่ายและระบบป้องกัน ยืนยันว่าไม่มี Traffic แปลกปลอมเล็ดลอดเข้าสู่วงเซิร์ฟเวอร์หลัก ฐานข้อมูล HOSxP ปลอดภัย ๑๐๐%
- ๑๔.๐๐ น. ทีม IT Support นำเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ทั้ง ๓ เครื่องออกจากระบบเครือข่าย เพื่อดำเนินการฟอร์แมต (Format) ฮาร์ดดิสก์แบบล้างข้อมูลขั้นเด็ดขาด (Secure Wipe) และติดตั้งระบบปฏิบัติการใหม่

๔.๔. การกู้คืนระบบ (Recovery)

- ๑๔.๓๐ น. จำลองการกู้คืนข้อมูลแฟ้มปฏิบัติงานของฝั่ง OPD โดยนายวชิรวิทย์ อุดมฉวี ทำการดึงข้อมูลย้อนหลัง (Restore) จากระบบ Proxmox Backup Server (PBS) ซึ่งเป็นระบบสำรองข้อมูลแบบ Air-Gapped การทดสอบกู้คืนข้อมูลสำเร็จลุล่วงภายในเวลา ๒๐ นาที ข้อมูลมีความสมบูรณ์
- ๑๕.๐๐ น. ทีมงานนำเครื่องคอมพิวเตอร์ที่ติดตั้งใหม่กลับเข้าสู่จุดบริการ และปลดล็อก Rule บน Firewall เพื่อให้ตึก OPD กลับมาใช้งานระบบ HOSxP ได้ตามปกติ

๔.๕. การรายงานผล (Post-Incident Activity & Reporting)

- ๑๕.๓๐ น. นางศิริกัญญา ถาบุตร รวบรวมข้อมูลทั้งหมด จำลองการเขียนรายงานเหตุการณ์ละเมิดความมั่นคงปลอดภัย เพื่อเตรียมนำเสนอผู้อำนวยการโรงพยาบาลภายใน ๒๔ ชั่วโมง และร่างหนังสือแจ้งเหตุต่อ สกมช. ภายในกรอบเวลา ๗๒ ชั่วโมง

๕. ตัวชี้วัดความสำเร็จของการฝึกซ้อม (Key Performance Indicators - KPIs) จากการประเมินผลการปฏิบัติงานตามสถานการณ์จำลอง พบว่าทีมงานสามารถบรรลุตัวชี้วัดที่ตั้งไว้ได้ ดังนี้

๕.๑. เวลาในการตอบสนองและกักกันภัย (Time to Contain) เป้าหมายภายใน ๓๐ นาที / ทำได้จริง ๒๐ นาที (ผ่านเกณฑ์)

๕.๒. ระยะเวลาที่ระบบหยุดชะงัก (Recovery Time Objective - RTO) เป้าหมายภายใน ๔ ชั่วโมง / ทำได้จริง ๒ ชั่วโมง (ผ่านเกณฑ์)

๕.๓. จุดสูญเสียของข้อมูล (Recovery Point Objective - RPO) เป้าหมายย้อนหลังไม่เกิน ๒๔ ชั่วโมง / ทำได้จริง ๐ ชั่วโมง (ไม่สูญเสียข้อมูลผู้ป่วย เนื่องจากป้องกันเซิร์ฟเวอร์หลักได้ทัน)

๖. บทเรียนที่ได้รับและข้อเสนอแนะ (Lessons Learned) คณะทำงานได้จัดทำ After Action Review (AAR) เพื่อสรุปจุดแข็งและจุดที่ต้องพัฒนา ดังนี้

จุดแข็งของระบบ (Strengths)

๑. ด้านบุคลากร (People) ทีมงานมีความตื่นตัว สื่อสารได้รวดเร็ว และเข้าใจบทบาทหน้าที่ของตนเองอย่างชัดเจน

๒. ด้านกระบวนการ (Process) แผนการตัดขาดเครือข่าย (Network Isolation) มีความชัดเจนและปฏิบัติได้ทันที

๓. ด้านเทคโนโลยี (Technology) การแบ่ง VLAN ร่วมกับนโยบายบน FortiGate และสถาปัตยกรรมจัดเก็บข้อมูลแบบ PBS มีความแข็งแกร่ง สามารถปกป้องข้อมูลสำคัญได้อย่างมีประสิทธิภาพ

จุดที่ต้องปรับปรุง (Areas for Improvement)

๑. ควรมีระบบตรวจจับและแจ้งเตือนความผิดปกติของเครือข่ายแบบอัตโนมัติ (Automated Alerting System) เพื่อลดภาระการเฝ้าระวังของเจ้าหน้าที่

๒. พฤติกรรมของผู้ใช้งาน (User Awareness) ยังเป็นช่องโหว่สำคัญ บุคลากรทางการแพทย์บางส่วนยังขาดความเข้าใจในการรับมือเมื่อพบหน้าจอผิดปกติ (เช่น เผลอปิดเครื่อง)

๗. แผนดำเนินการปรับปรุงและบทสรุปผู้บริหาร (Remediation Plan & Executive Summary) แผนดำเนินการระยะสั้น

ศูนย์เทคโนโลยีสารสนเทศจะจัดทำสื่อประชาสัมพันธ์ (Infographic) เรื่อง "ข้อควรปฏิบัติเมื่อพบไวรัสเรียกค่าไถ่" ติดตั้งเป็น Background หน้าจอคอมพิวเตอร์ของจุดบริการทุกจุด ภายในไตรมาสที่ ๒

สรุปผลต่อผู้บริหาร

การฝึกซ้อมแผนรับมือภัยคุกคามทางไซเบอร์ ประจำปี ๒๕๖๙ สำเร็จลุล่วงด้วยดี ระบบโครงสร้างพื้นฐานด้านไอทีของโรงพยาบาลพระอาจารย์มั่น ภูริทัตโต มีความพร้อมรับมือต่อสถานการณ์ฉุกเฉินระดับวิกฤต สามารถป้องกันความเสียหายต่อฐานข้อมูลผู้ป่วย และสามารถให้บริการทางการแพทย์ได้อย่างต่อเนื่องและปลอดภัย

ลงชื่อ.....

(นางศิริกัญญา ถาบุตร)

ผู้บัญชาการเหตุการณ์ / หัวหน้ากลุ่มงานฯ

วันที่ เดือน มีนาคม พ.ศ. ๒๕๖๙

ลงชื่อ.....

(นายพันธวี คำสาว)

ผู้อำนวยการโรงพยาบาลพระอาจารย์มั่น ภูริทัตโต

ผู้อนุมัติและรับทราบผลการฝึกซ้อม