รายงานการประเมินความเสี่ยงไซเบอร์ (Cybersecurity Risk Assessment Report)

วันที่ทำประเมิน : 23 มีนาคม 2569

ผู้จัดทำรายงาน : นายอิสระภาพ เบ้าน้อย

ชื่อระบบ : Critical Core Application Himpro

1. สรุปสำหรับผู้บริหาร (Executive Summary)

วันที่ทำการประเมิน : 23 มีนาคม 2569

วัตถุประสงค์ : การประเมินความเสี่ยงของระบบบริหารจัดการโรงพยาบาลโนนคูณ (Himpro) เพื่อระบุความเสี่ยงที่เกี่ยวข้องกับข้อมูลลูกค้าที่ใช้บริการ รวมถึงหาวิธีการควบคุมที่เหมาะสม

ประเภทของการประเมิน : การประเมินความเสี่ยงครั้งแรก

ระดับความเสี่ยงโดยรวม : ระดับความเสี่ยงโดยรวมถูกประเมินว่าอยู่ในระดับ สูง

จำนวนความเสี่ยงที่ระบุทั้งหมด : 16 รายการ

ความเสี่ยงที่ยอมรับได้ (ความเสี่ยงต่ำ) : 1 รายการ

ความเสี่ยงปานกลาง: 13 รายการ

ความเสี่ยงสูง: 2 รายการ

2. รายละเอียดของรายงาน (Body of the Report)

2.1 วัตถุประสงค์ของการประเมินความเสี่ยง

1. ประเมินความเสี่ยงของระบบบริหารจัดการโรงพยาบาลโนนคูณ (Himpro) ที่เกี่ยวข้องกับความลับ (Confidentiality), ความถูกต้อง (Integrity), และความพร้อมใช้งาน (Availability) ของผู้ใช้บริการ
2. ระบุความเสี่ยงที่อาจก่อให้เกิดปัญหากับระบบบริหารจัดการโรงพยาบาลโนนคูณ (Himpro) รวมถึงการจัดการข้อมูลลูกค้าที่มาใช้บริการ
3. ตรวจสอบการใช้มาตรการควบคุมเพื่อปกป้องระบบจากภัยคุกคามไซเบอร์

2.2 โมเดลความเสี่ยงและวิธีการประเมิน

ใช้โมเดลความเสี่ยงตาม NIST SP 800-30 Rev. 1 ซึ่งประเมินตามความรุนแรงและโอกาสของความเสี่ยง

โดยใช้คะแนนจาก 1 ถึง 5 (1 = ต่ำสุด, 5 = สูงสุด) และคำนวณคะแนนรวมเพื่อประเมินระดับความเสี่ยง

รายละเอียดความเสี่ยง (Detailed Risk Assessment) ในแต่ละ Cluster (เน้นเฉพาะ Cluster ที่มีระดับความเสี่ยงสูง เป็นหลัก

	ความเสี่ยง	ระดับความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	การควบคุมที่มีอยู่ปัจจุบัน	คำแนะนำเพิ่มเติม	คาดว่าจะเสร็จสิ้น
1	การโจมตีด้วยมัลแวร์ (Malware Attacks)	สูง	เสี่ยงการโจรกรรมข้อมูลการเงินหรือการเรียกค่าไถ่ (Ransomware) ระบบล่ม ทำให้สูญเสียรายได้ ข้อมูลลูกค้าหรือผู้ใช้บริการถูกขโมยทำให้สูญเสียความเชื่อมั่น ความน่าเชื่อถือขององค์กรลดลง	ติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ในทุกอุปกรณ์ใช้ระบบ Endpoint Security เพื่อสแกนหาไวรัสโดยใช้ระบบ IDS/IPS ตั้งค่าการอัปเดตอัตโนมัติ	ทดสอบระบบการป้องกันมัลแวร์อย่างสม่ำเสมอ, ดำเนินการ Penetration Testing เพื่อค้นหาช่องโหว่ที่อาจถูกใช้โจมตี, จัดอบรมเกี่ยวกับการหลีกเลี่ยงการดาวน์โหลดไฟล์หรือเข้าเว็บไซต์ที่ไม่น่าเชื่อถือ	31 ธ.ค.68
2	การโจมตีด้วยแรนซัมแวร์ (Ransomware Attacks)	สูง	ข้อมูลภายในระบบถูกเข้ารหัส ไม่สามารถเข้าถึงหรือใช้งานได้ ระบบงานสำคัญหยุดชะงัก (System Downtime) สูญเสียข้อมูลสำคัญขององค์กรหรือผู้รับบริการ อาจต้องเสียค่าไถ่ (Ransom) เพื่อกู้คืนข้อมูล ส่งผลกระทบต่อความเชื่อมั่นและภาพลักษณ์ขององค์กร	มีการสำรองข้อมูล (Backup) เป็นประจำและจัดเก็บแยกจากระบบหลัก ติดตั้ง Antivirus / Endpoint Protection ทุกเครื่อง มีการอัปเดตระบบปฏิบัติการและซอฟต์แวร์อย่างสม่ำเสมอ จำกัดสิทธิ์การเข้าถึงข้อมูลตามหน้าที่ (Access Control) ใช้ Firewall และระบบตรวจจับการบุกรุก (IDS/IPS)	ทดสอบการกู้คืนข้อมูล (Disaster Recovery Test) อย่างสม่ำเสมอ ใช้ระบบ **Offline Backup** หรือ Immutable Backup อบรมพนักงานเรื่องการระวัง Email Phishing / ไฟล์แนบ ปิดการใช้งาน Macro ในไฟล์ Office โดยค่าเริ่มต้น ใช้ Multi-Factor Authentication (MFA) สำหรับระบบสำคัญ ทำ Network Segmentation เพื่อลดการกระจายของมัลแวร์	

จึงเรียนมาเพื่อทราบ

นายอิสระภาพ เบ้าน้อย : นางพรรณี วรธรรม

นักวิชาการคอมพิวเตอร์ พยาบาลวิชาชีพชำนาญการพิเศษ

รับทราบ : .....

(นายธนสันตชัย พรหมบุตร)

นายแพทย์ชำนาญการพิเศษ รักษาการในตำแหน่ง

ผู้อำนวยการโรงพยาบาลโนนคูณ