โรงพยาบาลดอนมดแดง

Donmoddaeng Hospital

รายงานการประเมินความเสี่ยงไซเบอร์ (Cybersecurity Risk Assessment Report)

วันที่ทำประเมิน : 21 เมษายน 2569

ผู้จัดทำรายงาน : นายณรงค์ชัย สาระรัตน์ นักวิชาการคอมพิวเตอร์ชำนาญการ

ชื่อระบบ : All Critical Core Application เช่น HI

1. สรุปสำหรับผู้บริหาร (Executive Summary)

วันที่ทำการประเมิน : 21 เมษายน 2569

วัตถุประสงค์ : การประเมินความเสี่ยงของระบบบริหารจัดการโรงพยาบาล (HI) เพื่อระบุความเสี่ยงที่เกี่ยวข้องกับข้อมูลลูกค้าที่ใช้บริการ รวมถึงหาวิธีการควบคุมที่เหมาะสม

ประเภทของการประเมิน : การประเมินความเสี่ยงครั้งแรก

ระดับความเสี่ยงโดยรวม : ระดับความเสี่ยงโดยรวมถูกประเมินว่าอยู่ในระดับ สูง

จำนวนความเสี่ยงที่ระบุทั้งหมด : 16 รายการ

ความเสี่ยงที่ยอมรับได้ (ความเสี่ยงต่ำ) : 5 รายการ

ความเสี่ยงปานกลาง: 8 รายการ

ความเสี่ยงสูง: 3 รายการ

2. รายละเอียดของรายงาน (Body of the Report)

2.1 วัตถุประสงค์ของการประเมินความเสี่ยง

1. ประเมินความเสี่ยงของระบบบริหารจัดการโรงพยาบาล All Critical Core Application ที่เกี่ยวข้องกับความลับ (Confidentiality), ความถูกต้อง (Integrity), และความพร้อมใช้งาน (Availability) ของผู้ใช้บริการ
2. ระบุความเสี่ยงที่อาจก่อให้เกิดปัญหากับระบบบริหารจัดการโรงพยาบาล All Critical Core Application 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) ระบบล่มทำให้สูญเสียรายได้ ข้อมูลลูกค้าหรือผู้ใช้บริการถูกขโมยทำให้สูญเสียความเชื่อมั่น ความน่าเชื่อถือขององค์กรลดลง	ติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ในทุกอุปกรณ์ใช้ระบบ Endpoint Security เพื่อสแกนหาไวรัสโดยใช้ระบบ IDS/IPS ตั้งค่าการอัปเดตอัตโนมัติ	ทดสอบระบบการป้องกันมัลแวร์อย่างสม่ำเสมอ, ดำเนินการ Penetration Testing เพื่อค้นหาช่องโหว่ที่อาจถูกใช้โจมตี, จัดอบรมเกี่ยวกับการหลีกเลี่ยงการดาวน์โหลดไฟล์หรือเข้าเว็บไซต์ที่ไม่น่าเชื่อถือ	30 ก.ย.69
2	การโจมตีด้วยฟิชชิง (Phishing Attacks)	สูง	เสี่ยงการโจรกรรมข้อมูล ระบบล่มทำให้สูญเสียรายได้ ข้อมูลลูกค้าหรือผู้ใช้บริการถูกขโมยทำให้สูญเสียความเชื่อมั่น ความน่าเชื่อถือขององค์กรลดลง	ติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ในทุกอุปกรณ์ใช้ระบบ Endpoint Security เพื่อสแกนหาไวรัสโดยใช้ระบบ IDS/IPS ตั้งค่าการอัปเดตอัตโนมัติ	ทดสอบระบบการป้องกัน อย่างสม่ำเสมอ, ดำเนินการจัดอบรม จนท.ให้ตระหนักถึงความเสียหายที่อาจเกิดขึ้นและใช้อินเทอร์เน็ตด้วยความปลอดภัย	30 ก.ย.69
3	การโจมตีด้วยแรนซัมแวร์ (Ransomware Attacks)	สูง	เสี่ยงการโจรกรรมข้อมูล ระบบล่มทำให้สูญเสียรายได้ ข้อมูลลูกค้าหรือผู้ใช้บริการถูกขโมยทำให้สูญเสียความเชื่อมั่น ความน่าเชื่อถือขององค์กรลดลง	ติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ในทุกอุปกรณ์ใช้ระบบ Endpoint Security เพื่อสแกนหาไวรัสโดยใช้ระบบ IDS/IPS ตั้งค่าการอัปเดตอัตโนมัติ	ทดสอบระบบการป้องกัน อย่างสม่ำเสมอ, ดำเนินการจัดอบรม จนท.ให้ตระหนักถึงความเสียหายที่อาจเกิดขึ้นและใช้อินเทอร์เน็ตด้วยความปลอดภัย	30 ก.ย.69

จึงเรียนมาเพื่อทราบ

ลงชื่อ ผู้จัดทำ : นายณรงค์ชัย สาระรัตน์ นักวิชาการคอมพิวเตอร์ชำนาญการ

รับทราบ :

นายแพทย์วสุวัตติ์ พบลาภ
ตำแหน่ง ผู้อำนวยการโรงพยาบาลดอนมดแดง (CISO)