ฟอร์มสำหรับทำแผนรับมือ Business Continuity Plan (BCP) โรงพยาบาลอุดรธานี

เหตุการณ์: โดน ransomware attack ส่งผลให้ระบบบริการไม่สามารถดำเนินได้
วันที่: ๓๐ กันยายน ๒๕๖๗
แผนก: งานคลังพัสดุ กลุ่มงานพัสดุ
ผู้รับผิดชอบ: นายธนะเมศฐ์ ภามาตย์ชัยกุล และเจ้าหน้าที่งานคลังพัสดุ

๑. บทนำ

จากสถานการณ์ระบบคอมพิวเตอร์ของโรงพยาบาลอุดรธานี โดนโจมตีจาก ransomware attack ในวันที่ ๙ ธันวาคม ๒๕๖๖ งานคลังพัสดุ ได้จัดทำแผนวิเคราะห์ปัญหาและอุปสรรคจากการรับมือ ransomware attack ในครั้งนี้ เพื่อเตรียมพร้อมในการรับมือกับสถานการณ์ที่อาจเกิดขึ้น และใช้ในกรณีที่เกิดวิกฤติ หรือเหตุการณ์ฉุกเฉินต่าง ๆ ที่อาจจะเกิดขึ้นในอนาคต จากระบบเซิฟเวอร์ ระบบเน็ตเวิร์คขัดข้อง ระบบคอมพิวเตอร์ล่ม เพื่อให้ภารกิจของโรงพยาบาลมีความต่อเนื่อง ไม่หยุดชะงัก ไม่มีผลกระทบต่อการให้บริการผู้ป่วย สร้างความมั่นใจให้กับผู้ป่วย ปฏิบัติงานอย่างมีประสิทธิภาพและมีประสิทธิผล

ปัญหา

ระบุบทเรียนปัญหาจากเหตุการณ์ ransomware attack:

- ไม่สามารถใช้งาน อินเตอร์เน็ต ไม่สามารถใช้งานระบบฐานข้อมูลได้ หน่วยเบิก/กลุ่มงานไม่สามารถเข้าถึงข้อมูลการรับเข้าและจ่ายออกของวัสดุต่างๆ ผ่านระบบฐานข้อมูลได้

- วิเคราะห์สาเหตุของปัญหา: ระบบรักษาความปลอดภัย และระบบป้องกันไวรัสของโรงพยาบาลอุดรธานี ไม่รัดกุม โปรแกรมป้องกันมัลแวร์ไม่อัพเดต ขาดการเฝ้าระวัง เพราะเหตุเกิดในช่วงวันหยุดยาวหรือนอกเวลาราชการ มีเพียงเจ้าหน้าที่ที่ขึ้นเวร ทำให้ตรวจสอบแก้ไข สถานการณ์ที่เกิดขึ้นไม่ทันการณ์ ระบบการสำรองข้อมูลที่มีอาจไม่เพียงพอ ไม่สามารถแบ่งเป็นหน่วยงานเอกเทศ ๑:๑ ได้สำหรับการเก็บสำรองข้อมูล อีกทั้งบุคลากรไม่มีความรู้เพียงพอและไม่เคยเกิดเหตุการณ์นี้ขึ้น ทำให้ไม่สามารถป้องกันระบบ ทำให้เกิดภัยคุกคามทางไซเบอร์ได้และใช้ระยะเวลาในการเข้าจู่โจมไม่นาน

ระบุแนวทางการแก้ไขปัญหา:

- จัดทำข้อมูลการเบิก - จ่าย ด้วยมือ (ใบเบิก ๓ สี) และสต๊อกการ์ด

อุปสรรค

ระบุอุปสรรคที่เกิดขึ้นในการรับมือกับ ransomware attack:

- บุคลากรขาดความรู้ ความเข้าใจ และแผนการรับมือต่อการเกิด ransomware ขาดการจัดฝึกอบรม การสร้างความเข้าใจและแนวทางการรับมือต่อการเกิด ransomware ให้แก่เจ้าหน้าที่ในหน่วยงานรับทราบ

ระบุแนวทางการแก้ไขอุปสรรค:

- จัดฝึกอบรมให้ความรู้และเตรียมพร้อม ในการรับมือต่อการเกิด ransomeware พร้อมซ้อมแผนการปฏิบัติงานหากเกิดขึ้นจริง

- ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งาน ของผู้ใช้งาน จำกัดการเข้า web site ที่ไม่เกี่ยวข้องการทำงานของตนเองเพื่อป้องกันการไปดาวน์โหลดเอกสาร หรือไฟล์อื่น ๆ ที่ไม่จำเป็น

- กำหนดหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานในระบบสารสนเทศ ทบทวนสิทธิ์การเข้าถึงข้อมูลอย่างสม่ำเสมอ

- จัดการฝึกอบรมและสร้างความตระหนักในโรงพยาบาล เกี่ยวกับการทำความเข้าใจและป้องกัน ransomware attack พร้อมให้ทุกคนได้ซ้อมแผนปฏิบัติจริง เพื่อให้เกิดการตื่นตัว และทราบขั้นตอนที่ถูกต้อง หากเกิดเหตุการณ์ขึ้นจริง

- แจ้งให้ผู้รับบริการทราบถึงปัญหาที่เกิดขึ้นเมื่อมีผู้มารับบริการหน้าช่องรับชำระเงิน กล่าวขอโทษและแจ้งว่าอยู่ระหว่างการดำเนินการแก้ไขข้อมูล

- แจ้งขั้นตอนการรับบริการในครั้งถัดไปให้นำบัตรประชาชน ยา เอกสาร ที่เกี่ยวข้องมาด้วยทุกครั้ง

๒. รายละเอียดแผน BCP

๒.๑ ผลกระทบ

ระบุผลกระทบของ ransomware attack ที่มีต่องานบริการของแผนก :

- ทำให้ไม่สามารถดูข้อมูลต่างๆ เช่นการรับเข้า จ่ายออก ในระบบได้

ระบุผลกระทบต่อผู้ป่วย ญาติ และบุคลากร :

- หน่วยเบิกไม่สามารถดำเนินการเบิกวัสดุต่างๆ ผ่านระบบได้

๒.๒ กลยุทธ์

ระบุกลยุทธ์ที่จะใช้ในการรับมือกับ ransomware attack :

- ใช้ซอฟต์แวร์ที่ทำหน้าที่ตรวจสอบการผ่านเข้า ออก คัดกรองข้อมูลที่เข้ามาว่าเป็นข้อมูลอะไรจากไหน ส่งไปไหน ปลอดภัยหรือไม่

- ใช้ซอฟต์แวร์ที่ตรวจจับความผิดปกติที่เกิดขึ้นกับเครือข่ายคอมพิวเตอร์ หากมีความผิดปกติให้มีสัญญาณแจ้งเตือนเหตุภัยคุกคามทางไซเบอร์ โดยให้ระบบตรวจจับและป้องกันการบุกรุก หรือสัญลักษณ์แจ้งบอก โดยให้เจ้าหน้าที่ทุกท่านในโรงพยาบาลทราบเป็นอย่างดี เพื่อให้ช่วยกันเฝ้าระวัง ป้องกัน แก้ไข เมื่อเกิดเหตุการณ์ถูกโจมตีทางไซเบอร์ ปิดระบบได้ทันการณ์

- มีการใช้ Software ซึ่งประกอบด้วย Server ๒ เครื่อง เมื่อตัวใดตัวหนึ่งมีปัญหา อีกเครื่องจะทำงานทดแทนได้ทันที
- มีการกำหนดเวลาการสำรองข้อมูลอัตโนมัติทุกวัน
- มีการติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ในระบบคอมพิวเตอร์

ระบุวิธีการที่จะรักษางานบริการที่จำเป็น :

แต่ละหน่วยงาน - หน่วยงานจัดทำระบบสำรองข้อมูลในระบบ Cloud เพื่อให้การดำเนินงานเป็นไปอย่างต่อเนื่องแยกพื้นที่การจัดเก็บของ พร้อมทั้งตั้งระบบป้องกันไวรัสและกำหนดเวลาการสำรองข้อมูลอัตโนมัติทุกวัน

ระบุวิธีการที่จะลดผลกระทบต่อผู้ป่วย ญาติ และบุคลากร :

- ดำเนินการเบิก – จ่าย วัสดุต่าง ๆ ด้วยมือ โดยใช้ใบเบิก ๓ สี และบันทึกการเบิกจ่ายด้วยมือ ลง สต๊อกการ์ด

๒.๓ แผนปฏิบัติการ

ระบุขั้นตอนที่ชัดเจนในการรับมือกับ ransomware attack :

๑. ปิดเครื่องไว้/สำรองข้อมูล/ส่งออกไปเก็บไว้ที่อีเมลล์

๒. ปฏิบัติตามแนวทาง Cyber security (Policy การใช้งาน Internet แบ่งเป็น ๓ กลุ่ม)

๒.๑ กลุ่มที่ ๑ Lan only ห้ามเข้าถึง Internet เด็ดขาด Ex. ห้องตรวจ,โต๊ะซักประวัติ,ห้องแล็ป,ห้องจ่าย,งานเวชระเบียน

๒.๒ กลุ่มที่ ๒ Lan + เฉพาะเว็บที่อนุญาตเกี่ยวข้องกับการทำงาน Ex. ลงทะเบียนตรวจสิทธิ์,การเงิน,งานประกันสุขภาพ

๒.๓ กลุ่มที่ ๓ Internet only ห้ามเข้าถึง Lan รพ.เด็ดขาด Ex. เครื่องที่ไม่มีโปรแกรมโรงพยาบาล,เครื่อง Stand alone

๓. ไม่ต่อ Handy drive

ระบุผู้รับผิดชอบสำหรับแต่ละขั้นตอน :

๑. การฝึกฝนและสร้างความตระหนักรู้ : กลุ่มงานเทคโนโลยีสารสนเทศ

๒. การแยกเครือข่ายในการใช้งาน :

๓. การสำรองข้อมูล : งานศูนย์คอมพิวเตอร์

ระบุเวลาที่คาดว่าจะใช้ในการดำเนินการแต่ละขั้นตอน :

๑. การจัดฝึกอบรม : ระยะเวลา ๑ วัน

๒. การสำรองข้อมูล : สำรองข้อมูลทุกวัน เวลา ๒๔.๐๐ น.

๓. การดำเนินการแก้ไข / ตรวจสอบ ๑ วัน

๒.๔ ทรัพยากร

ระบุทรัพยากรที่จำเป็นในการดำเนินการแผน BCP :

๑. บุคลากรในหน่วยงาน

๑.๑. ให้ความรู้เพื่อให้บุคลากรของโรงพยาบาลอุดรธานีตระหนักถึงภัยคุกคาทางไซเบอร์โดยต้องดำเนินการจัดฝึกบรมให้ความรู้แก่บุคลากรภายในเพื่อลดความเสี่ยงจากภัยไซเบอร์

๑.๒. การแจ้งรายชื่อเจ้าหน้าที่สำหรับประสานงานด้านการรักษาความมั่นคง ปลอดภัย ทางไซเบอร์ ในการประสานงาน

๑.๓. จัดให้มีผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ เพื่อให้เห็นความผิดปกติที่เกิดขึ้นในระหว่างวันหยุดราชการ หรือเวลานอกราชการ

๑.๔. ให้ความรู้ และฝึกอบรมเฉพาะทางด้านความปลอดภัยทางไซเบอร์ให้บุคลากรที่ดูแลด้านการรักษาความปลอดภัยของเครือข่าย เมื่อได้รับรายงานแล้วจะต้องมีการตรวจสอบข้อเท็จจริงหรือยืนยันข้อมูลทุกครั้ง

๒. ระบบสำรองข้อมูล

ในกรณีที่ภัยคุกคามทางไซเบอร์ก่อเกิดความเสียหายแก่ระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานอย่างมากจนไม่สามารถทำงานได้เป็นเวลานาน โรงพยาบาลอุดรธานี ควรพิจารณาทางเลือกการแก้ไขปัญหาโดยการกู้คืนข้อมูลที่เสียหาย และสำรองข้อมูลทาง แฮนดี้ไดร์ฟ หรือส่งข้อมูลสำรองทาง เมลล์ พร้อมมีการการใช้ Software ซึ่งประกอบด้วย Server ๒ เครื่อง เมื่อตัวใดตัวหนึ่งมีปัญหา อีกเครื่องจะทำงานทดแทนได้ทันที มีการกำหนดเวลาการสำรองข้อมูลอัตโนมัติทุกวัน และมีการติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ในระบบคอมพิวเตอร์

๓. ระบบการตรวจสอบและการเฝ้าระวัง

มีระบบตรวจจับและป้องกันการบุกรุก โดยใช้ในการระบุเหตุการณ์ที่น่าสงสัยว่าอาจเป็นภัยคุกคามและบันทึกข้อมูลที่เกี่ยวข้อง รวมถึงวันที่ และเวลาที่ตรวจพบการโจมตี ประเภทการโจมที ที่อยู่ต้นทางและปลายทาง ชื่อผู้ใช้งาน ดังนั้น ข้อมูลลักษณะเฉพาะของการโจมตีต้องได้รับการอัพเดตอย่างสม่ำเสมอ เพื่อให้สามารถตรวจพบการโจมตีรูปแบบใหม่ ๆ ได้ ต้องให้เกิดการแจ้งเตือนในเวลาที่ผิดพลาดได้ โดยให้มีการแจ้งเตือนด้วยเสียงสัญญาณดัง ๆว่ามีกิจกรรมที่เป็นอันตรายกำลังเกิดขึ้น

-หรือมีการใช้บริการจ้างเหมาเฝ้าระวังภัยคุกคามจากผู้ให้บริการภายนอก /บริษัทเอกชน

๒.๕ การทดสอบและฝึกอบรม

ระบุวิธีการทดสอบแผน BCP :

มีการทดสอบแผนบริหารความต่อเนื่องฯ เป็นประจำทุกปีเพื่อให้มั่นใจว่าโรงพยาบาลอุดรธานีมีการเตรียมตัวและมีความสามารถในการกู้คืนข้อมูลภายในระยะเวลาที่กำหนดไว้

ระบุวิธีการฝึกอบรมบุคลากรให้สามารถปฏิบัติตามแผน BCP ได้ :

๑. สร้างสถานการณ์จำลองเป็นประจำทุกปีต้องมีการปรับเปลี่ยนหมุนเวียนสถานการณ์เพื่อให้มีการทดสอบความสูญเสีย ทุกๆ ปี

๒. สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ มีการฝึกอบรมให้กับผู้บริหาร ข้าราชการ ลูกจ้าง อย่างน้อยปีละ ๑ ครั้ง

สรุปประเด็นที่ควรดำเนินการ

สรุปประเด็นที่ควรดำเนินการ	U	S	I
การป้องกัน			
๑.การติดตั้งและอัพเดตซอฟต์แวร์และระบบปฏิบัติการ			/
๒.การกำหนดสิทธิ์ในการเข้าถึงข้อมูลในองค์กร โดยจำกัดสิทธิ์ให้เฉพาะผู้ที่จำเป็น		/	/
๓.การกำหนดนโยบายการใช้งานและประกาศเผยแพร่การระงับกิจกรรมที่ไม่จำเป็น			/
การเตรียมความพร้อมเพื่อรับสถานการณ์เมื่อเกิดเหตุ			
๑.การฝึกอบรมและการทดสอบความรู้	/	/	/
๒.การจำลองสถานการณ์	/	/	/
การปฏิบัติระหว่างเกิดเหตุเพื่อให้การบริการดำเนินต่อไปได้			
๑.จัดหาคอมพิวเตอร์ส่วนบุคคลที่ไม่มีการเชื่อมต่อกับระบบของโรงพยาบาล	/		
๒.การเชื่อมต่ออินเทอร์เน็ตผ่านมือถือส่วนบุคคลโดยใช้ Wi-Fi ฮอตสปอต	/		
๓.การสำรองข้อมูลในระบบ Cloud ของหน่วยงาน			
การปฏิบัติหลังระบบกลับสู่ปกติ			
๑.การฝึกฝนและสร้างความตระหนักรู้		/	/
๒.การแยกเครือข่ายในการใช้งาน			/
๓.การสำรองข้อมูล	/		/

U =ดำเนินการได้เองระดับหน่วยงาน

S = ต้องคุยเชิงระบบเพื่อทำงานให้สอดคล้องกัน

I = ต้องได้รับการสนับสนุนจาก IT