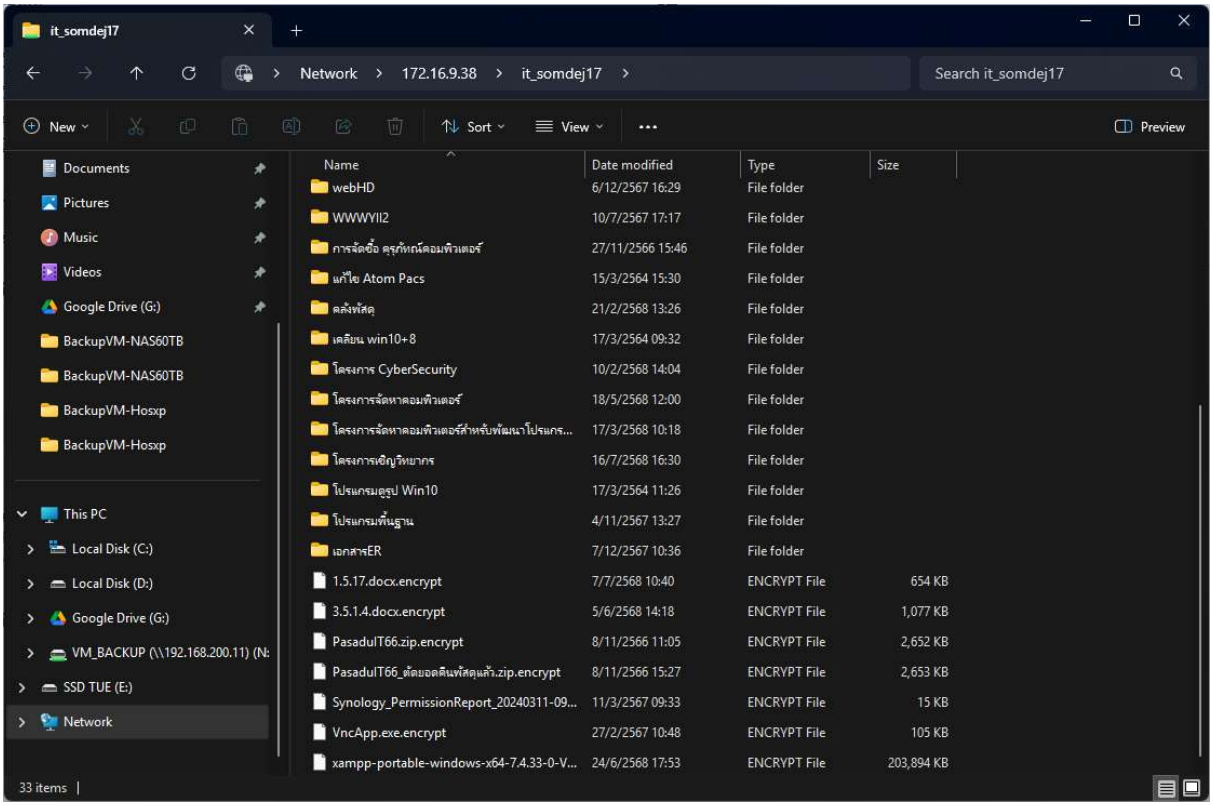
9.6.3 มีการฝึกซ้อม และทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ (INCIDENT RESPONSE PLAN) อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

จากสถานการณ์จริง โรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 **ติดไวรัส Ransomware เมื่อวันที่ 10 มิถุนายน 2568 เวลา 14:26 น.** จากการตรวจพบ มีการเข้ารหัสไฟล์ .encrypt ครั้งแรกในอุปกรณ์ **NAS รุ่น Synology DiskStation DS925+**



ต่อมาพบการแพร่กระจายของไวรัสไปยังโฟลเดอร์ต่าง ๆ ภายในอุปกรณ์ NAS และเกิดการเข้ารหัสไฟล์จำนวนมากในวันที่ 11 มิถุนายน 2568 เวลา 00:11 น. ส่งผลให้พื้นที่จัดเก็บข้อมูลเต็ม และระบบ Shut Down ใช้งานไม่ได้

วิเคราะห์สาเหตุและสถานการณ์การแพร่กระจายของไวรัส คือ

1.มีการนำ Flash Drive จากภายนอกมาใช้งาน โดยไม่มีโปรแกรม Antivirus บนเครื่องคอมพิวเตอร์ของผู้ใช้ ทำให้ไวรัสสามารถเข้าสู่ระบบได้ และพยายามเชื่อมต่อไปยัง NAS Synology DS925+

2.การกำหนดสิทธิ์ของ User ไม่เหมาะสม พบว่า User ที่มีสิทธิ์ระดับ Admin สามารถเข้าถึงทุกโฟลเดอร์ภายใน NAS ซึ่งเอื้อต่อการแพร่กระจายของไวรัส

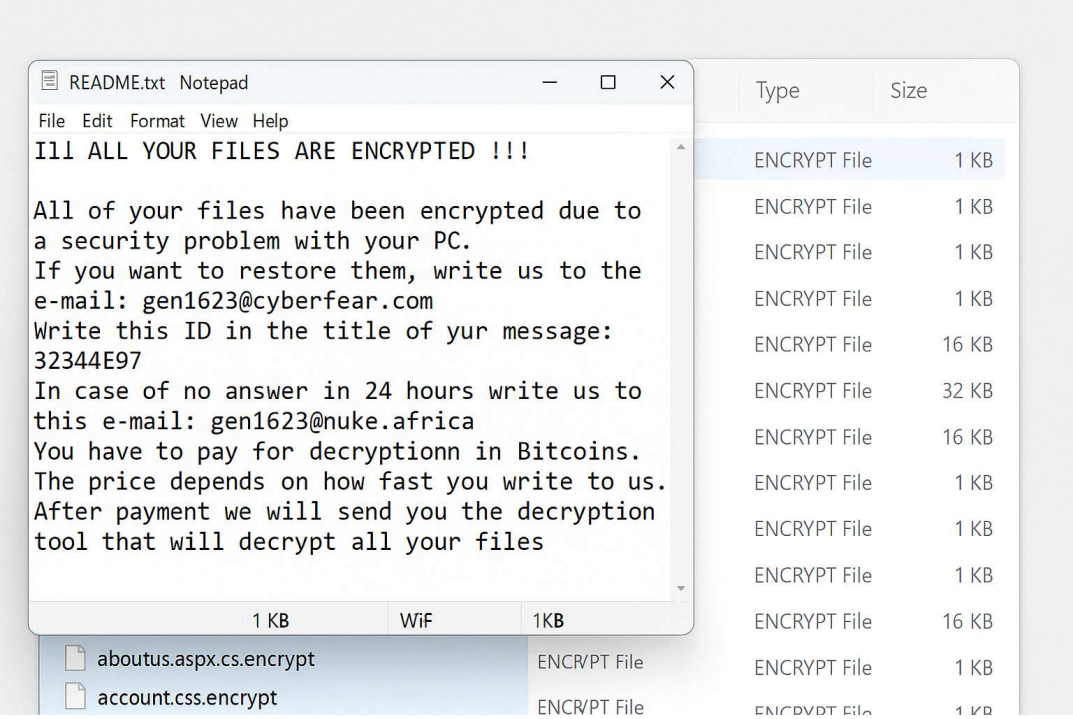
3.อุปกรณ์ NAS รุ่น Synology DS925+ ไม่สามารถติดตั้ง Antivirus ได้ ไม่มีระบบเตือนภัย หรือการป้องกันเพียงพอ อีกทั้งไม่มีการสำรองข้อมูลประจำวัน (ทำได้เพียงเดือนละ 1 ครั้งเท่านั้น)

5.ยังไม่มีการแยก VLAN สำหรับกลุ่มผู้ใช้งานออกจากกลุ่ม Server อย่างครบถ้วน ทำให้ไวรัสแพร่กระจายได้อย่างรวดเร็ว

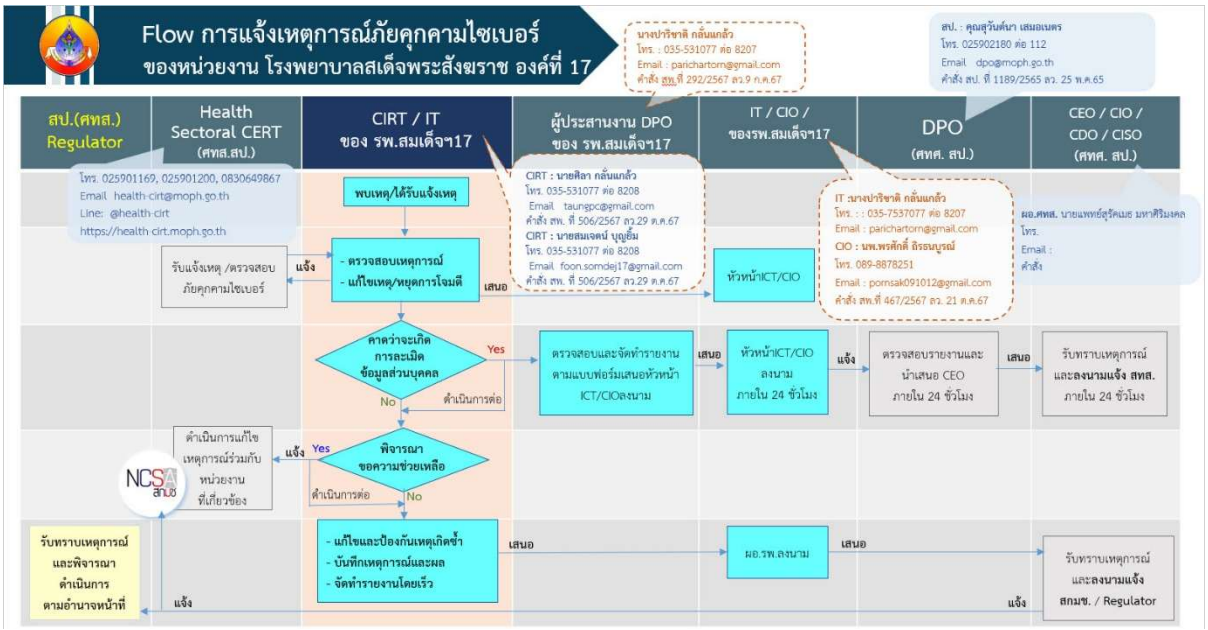
ขั้นตอนการดำเนินการแก้ไข Ransomware

1.ถอดสาย LAN ตัดการเชื่อมต่ออุปกรณ์ NAS Synology DS925+ ออกจากระบบเครือข่ายหลัก แล้วนำเครื่องคอมพิวเตอร์โน้ตบุ๊กเชื่อมต่อโดยตรง เพื่อตรวจสอบและกู้ข้อมูล

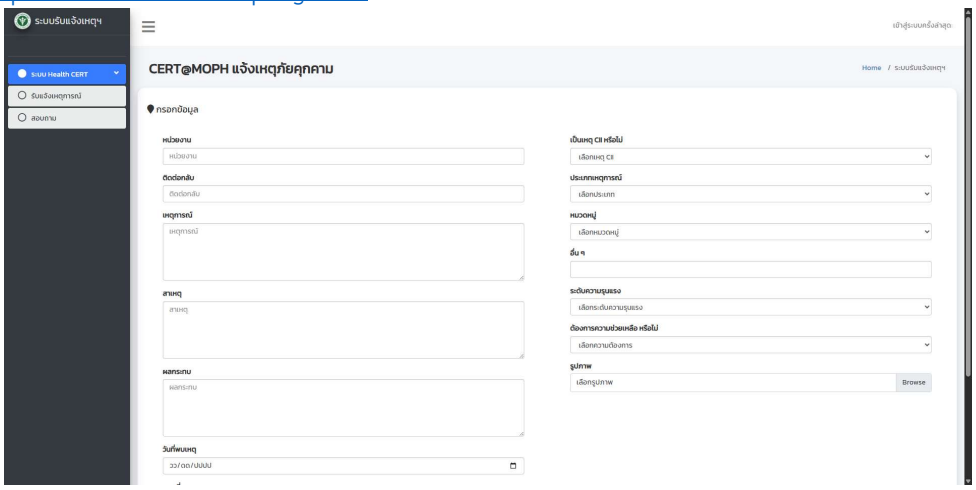
2.วิเคราะห์สาเหตุและตรวจสอบข้อมูลภายใน NAS พบว่าไฟล์ถูกเข้ารหัสและมีข้อความเรียกค่าไถ่แนบมาในบางโฟลเดอร์



3.โทรแจ้งรายงานสถานการณ์ภัยไซเบอร์ ให้หัวหน้ากลุ่มงาน หรือผู้อำนวยการโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 ทราบ และแจ้งให้ สสจ.สุพรรณบุรี รับทราบ



4.แจ้งเหตุ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CERT) ทางเว็บไซต์ https://health-cirt.moph.go.th/



5.ดำเนินการตามหลักการกู้ข้อมูล

5.1 เปลี่ยนรหัสผ่านการเข้าใช้งานอุปกรณ์ NAS Synology DS925+

5.2 สำรองข้อมูลที่สามารถกู้คืนได้ไปยังอุปกรณ์สำรองอื่น

5.3 ทำการ Format อุปกรณ์ NAS Synology DS925+

5.4 นำไฟล์ข้อมูลจาก External Hard Disk ที่สำรองไว้กลับมาใส่ในระบบใหม่

5.5 เปลี่ยนรหัสผ่านผู้ใช้งานทั้งหมด และกำหนดสิทธิ์เฉพาะเท่าที่จำเป็น

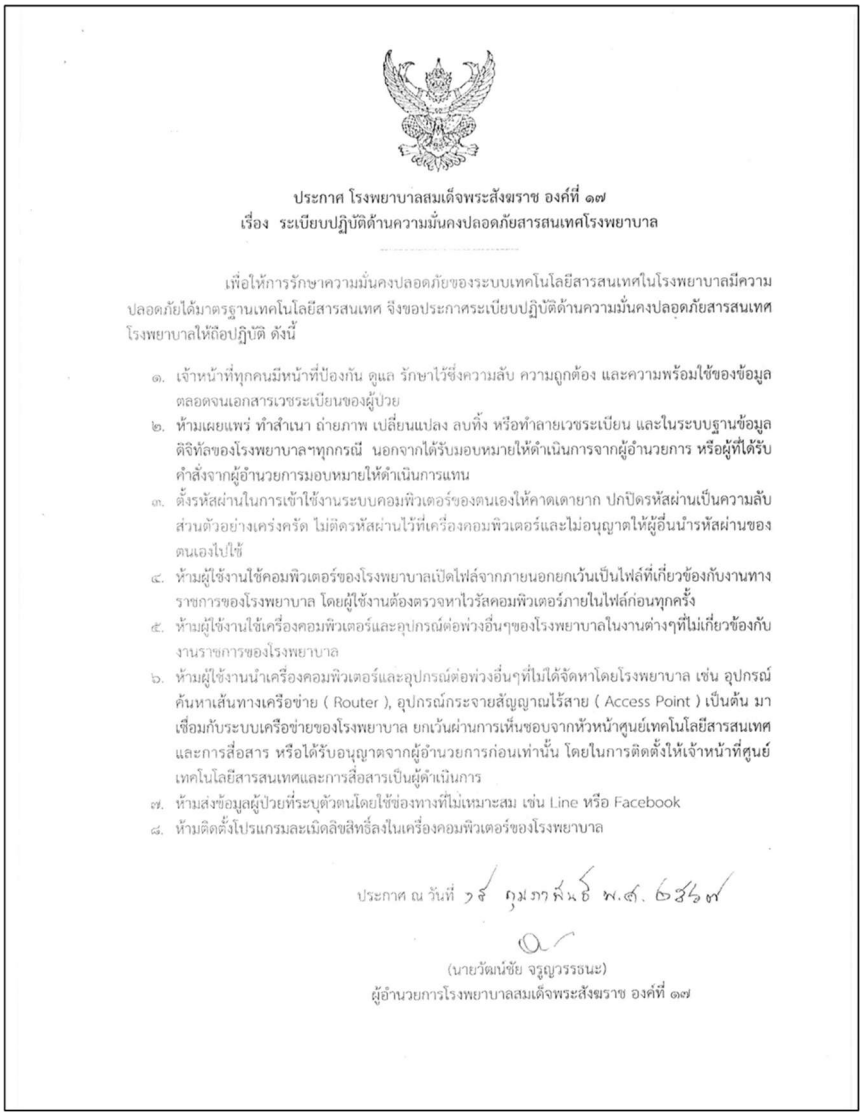
5.6 ตรวจสอบไวรัส Ransomware จากเครื่อง Client โดยวิเคราะห์จาก Firewall Log พบพฤติกรรมเสี่ยงจำนวน 3 เครื่อง

- ตัดการเชื่อมต่อ LAN
- ลง Windows ใหม่
- ติดตั้ง Antivirus แบบ EDR ป้องกันการติดไวรัสซ้ำ

6.รายงานสถานการณ์ต่อคณะกรรมการบริหารโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 และวางแผนติดตามความคืบหน้าอีกครั้งภายใน 30 วัน

7.ทำเอกสาร ตามแบบฟอร์ม แบบฟอร์มรายงานเหตุภัยคุกคามทางไซเบอร์ ให้ 2 หน่วยงาน รับทราบ คือ สกมช. อีเมล thaicert@ncsa.or.th และ ศทส.สป.สธ. อีเมล health-cirt@moph.go.th

8.สื่อสารให้เจ้าหน้าที่รับทราบแนวปฏิบัติด้านความมั่นคงปลอดภัยของโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 พร้อมสร้างความตระหนัก และขอความร่วมมือในการป้องกันไวรัสอย่างเข้มงวด



ประกาศ โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗
เรื่อง ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศโรงพยาบาล

เพื่อให้การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศในโรงพยาบาลมีความปลอดภัยได้มาตรฐานเทคโนโลยีสารสนเทศ จึงขอประกาศระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศโรงพยาบาลให้ถือปฏิบัติ ดังนี้

๑. เจ้าหน้าที่ทุกคนมีหน้าที่ป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลตลอดจนเอกสารเวชระเบียนของผู้ป่วย
๒. ห้ามเผยแพร่ ทำสำเนา ถ่ายภาพ เปลี่ยนแปลง ลบทิ้ง หรือทำลายเวชระเบียน และในระบบฐานข้อมูลดิจิทัลของโรงพยาบาลฯทุกกรณี นอกจากได้รับมอบหมายให้ดำเนินการจากผู้อำนวยการ หรือผู้ที่ได้รับคำสั่งจากผู้อำนวยการมอบหมายให้ดำเนินการแทน
๓. ตั้งรหัสผ่านในการเข้าใช้งานระบบคอมพิวเตอร์ของตนเองให้คาดเดายาก ปกปิดรหัสผ่านเป็นความลับส่วนตัวอย่างเคร่งครัด ไม่ติดรหัสผ่านไว้ที่เครื่องคอมพิวเตอร์และไม่อนุญาตให้ผู้อื่นนำรหัสผ่านของตนเองไปใช้
๔. ห้ามผู้ใช้งานใช้คอมพิวเตอร์ของโรงพยาบาลเปิดไฟล์จากภายนอกยกเว้นเป็นไฟล์ที่เกี่ยวข้องกับงานทางราชการของโรงพยาบาล โดยผู้ใช้งานต้องตรวจหาไวรัสคอมพิวเตอร์ภายในไฟล์ก่อนทุกครั้ง
๕. ห้ามผู้ใช้งานใช้เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นๆของโรงพยาบาลในงานต่างๆที่ไม่เกี่ยวข้องกับงานราชการของโรงพยาบาล
๖. ห้ามผู้ใช้งานนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นๆที่ไม่ได้จัดหาโดยโรงพยาบาล เช่น อุปกรณ์ค้นหาเส้นทางเครือข่าย (Router), อุปกรณ์กระจายสัญญาณไร้สาย (Access Point) เป็นต้น มาเชื่อมกับระบบเครือข่ายของโรงพยาบาล ยกเว้นผ่านการเห็นชอบจากหัวหน้าศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือได้รับอนุญาตจากผู้อำนวยการก่อนเท่านั้น โดยในการติดตั้งให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้ดำเนินการ
๗. ห้ามส่งข้อมูลผู้ป่วยที่ระบุตัวตนโดยใช้ช่องทางที่ไม่เหมาะสม เช่น Line หรือ Facebook
๘. ห้ามติดตั้งโปรแกรมละเมิดลิขสิทธิ์ลงในเครื่องคอมพิวเตอร์ของโรงพยาบาล

ประกาศ ณ วันที่ ๒๕ กุมภาพันธ์ พ.ศ. ๒๕๖๗

(นายวัฒน์ชัย จรูญวรรธนะ)
ผู้อำนวยการโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗