ที่ ศก ๒๐๓๒/ว ๓๙๓

สำนักงานสาธารณสุขอำเภอพยุห์
ถนนเฉลิมพระเกียรติ ร.๙ ต.พยุห์
ศก. ๓๓๒๓๐

๑๕ กันยายน ๒๕๖๓

เรื่อง การสำรองฐานข้อมูลโปรแกรม JHCIS

เรียน ผู้อำนวยการโรงพยาบาลส่งเสริมสุขภาพตำบลทุกแห่ง

เนื่องจากสถานการณ์การถูกโจมตีระบบคอมพิวเตอร์ ในโรงพยาบาลสระบุรี และอื่นๆ จาก ไวรัสประเภท แรนซัมแวร์ (Ransomware) ซึ่งมีจุดมุ่งหมายในการเรียกค่าไถ่ไฟล์ โดยการเข้ารหัส ได้แพร่ระบาดอยู่ในขณะนี้ ทำให้เกิดความเสียหายต่อระบบคอมพิวเตอร์

ในการนี้ สำนักงานสาธารณสุขอำเภอพยุห์ จึงขอให้ท่านได้ดำเนินการจัดเก็บไฟล์ฐานข้อมูล และข้อมูลที่มีความสำคัญของท่าน ไว้ในระบบที่ปลอดภัยมากว่า ๑ แหล่ง เพื่อป้องกันการถูกโจมตีจากไวรัสดังกล่าว และได้แนบวิธีป้องกันการแพร่ระบาดของไวรัสมาพร้อมแล้วนี้

จึงเรียนมาเพื่อทราบ และพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายฤทธิรงค์ โนนใหญ่)
สาธารณสุขอำเภอพยุห์

กลุ่มงานบริหารงานทั่วไป
งานเทคโนโลยีสารสนเทศ
โทร. ๐ ๔๕๘๑ ๓๕๙๘

วิธีป้องกันการแพร่ระบาดของไวรัส Ransomware

Ransomware คืออะไรและมีวิธีป้องกันได้อย่างไร

Ransomware หรือ มัลแวร์เรียกค่าไถ่ ชื่อที่หลายคนอาจจะเคยได้ยินมาบ้าง หรือแม้กระทั่งบางคนเคยโดนภัย Ransomware มากับตัวเอง โดยพฤติกรรมของ Ransomware มักจะทำการ Lock file หรือ encryption file เพื่อไม่ให้เหยื่อเข้าใช้งานไฟล์ที่ถูก Lock ไว้ได้ จากนั้นจะมีข้อความเพื่อทำการเรียกค่าไถ่ข้อมูลที่ได้ Lock ไว้ หากเหยื่อยินยอมจ่ายค่าไถ่แฮกเกอร์ก็จะปลดล็อคให้ แต่ในระยะหลังเริ่มมีการขู่ว่าจะปล่อยข้อมูลสู่สาธารณะดังเช่น ในข่าว ขู่ปล่อยข้อมูล Ransomware ที่ทำมากกว่ามัลแวร์เรียกค่าไถ่ หรือ นำไปประมูลขาย เช่น ข่าว DoppelPaymer อ้างเข้าถึงข้อมูลบริษัทผู้ดูแลระบบไอทีให้กับ NASA ได้ เป็นต้น

โดยส่วนใหญ่การที่จะตกเหยื่อของ Ransomware นั้นจะมีสาเหตุมาจากการที่ผู้ใช้งานดาวน์โหลดไฟล์ผ่านทางเว็บไซต์ที่ไม่น่าเชื่อถือและเป็นอันตราย เมื่อดาวน์โหลดมาแล้วกลับได้ Ransomware มาแทน ซึ่ง โดยหลักแล้ว Ransomware มักจะมุ่งเน้นโจมตีผ่านระบบปฏิบัติการ Microsoft Windows แต่ผลของการเข้า Lock ไฟล์นั้น สามารถลามไป Online Storage ต่าง ๆ ได้ด้วย

๑. วิธีการป้องกัน Ransomware สำหรับผู้ใช้งานทั่วไป (End user)

- เมื่อพบ website, link, file ที่ไม่น่าไว้ใจ ให้รีบลบทิ้ง ไม่ควรลองคลิกดูเพื่อทดสอบว่าเป็นโปรแกรมอะไร
- ติดตั้ง Antivirus หมั่น update และ scan อยู่เสมอ
- ทำการ backup file สำคัญไว้หลายๆ ที่โดยเฉพาะควรสำรองข้อมูลแบบออฟไลน์ด้วย เช่น copy ไฟล์เก็บไว้ใน Harddisk หรือ แฟลชไดร์ฟ เป็นต้น

๓. สิ่งที่ควรทำทุกเดือน (End user/Admin)

- ตรวจสอบทุกเดือน เช่น ช่องโหว่ของ OS และ หมั่น Update Patch สม่ำเสมอ
- กำหนดสิทธิ์การเข้าถึงไฟล์ที่สำคัญให้ได้เพียง Read-only เท่านั้น และหมั่นตรวจสอบการเข้าถึงไฟล์หรือ Folder เมื่อไม่มีการใช้งาน ให้ยกเลิกการแชร์ไฟล์ด้วย
- ไฟล์หรือ Folder ที่สำคัญ ให้กำหนดสิทธิ์การเข้าถึงจากบุคคลภายนอกให้เพียง Read only เท่านั้น

ที่มา https://www.catcyfence.com/it-security/article/what-is-ransomware-and-how-to-protect/
บริษัท กสท โทรคมนาคม จำกัด (มหาชน)