ด่วนที่สุด

ที่ สธ ๐๒๐๒/ว ๗๖๓๘

สำนักงานปลัดกระทรวงสาธารณสุข
ถนนติวานนท์ จังหวัดนนทบุรี ๑๑๐๐๐

๑๖ พฤษภาคม ๒๕๖๐

เรื่อง มาตรการป้องกัน Ransomware ชื่อ WannaCry สำหรับกระทรวงสาธารณสุข

เรียน อธิบดีทุกกรม/เลขาธิการคณะกรรมการอาหารและยา/นายแพทย์สาธารณสุขจังหวัด/ผู้อำนวยการโรงพยาบาลศูนย์/ทั่วไป/ผู้อำนวยการสำนัก/กอง/กลุ่ม ในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ทุกแห่ง

สิ่งที่ส่งมาด้วย แนวทางปฏิบัติตามมาตรการป้องกัน Ransomware ชื่อ WannaCry จำนวน ๑ หน้า

ตามที่มีการแพร่กระจายของมัลแวร์เรียกค่าไถ่ “WannaCry” โจมตีเครื่องคอมพิวเตอร์ทั่วโลก ส่งผลกระทบให้ธุรกิจและบริการ ร่วมถึงสถานพยาบาลหลายแห่งต้องหยุดบริการและต้องสูญเสียเงินจำนวนมากเพื่อจ่ายเป็นค่าไถ่คืนข้อมูลสำคัญ ซึ่งต้องจ่ายด้วยเงินสกุลดิจิทัล “บิตคอยน์” ทำให้ตามจับผู้รับเงินดังกล่าวไม่ได้นั้น

ในการนี้สำนักงานปลัดกระทรวงสาธารณสุข มีความกังวัลเกี่ยวกับเครื่องมือแพทย์ที่ใช้กันอยู่ในปัจจุบัน บางเครื่องอาจจะใช้ระบบปฏิบัติการ Windows จึงขอให้ทุกหน่วยงานในสังกัดกระทรวงสาธารณสุข ตระหนักและปฏิบัติตามมาตรการป้องกัน Ransomware ชื่อ WannaCry อย่างเคร่งครัด มิให้ตกเป็นเหยื่อของ Ransomware ชื่อ WannaCry โดยได้แนบแนวทางปฏิบัติตามมาตรการป้องกัน Ransomware ชื่อ WannaCry ตามสิ่งที่ส่งมาด้วย ทั้งนี้หากหน่วยงานต้องการความช่วยเหลือรวมถึงคำปรึกษา ติดต่อศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุขได้ตลอดเวลาที่โทร ๐ ๒๕๙๐ ๑๑๖๙, ๑๒๐๑ email: ict-moph@health.moph.go.th

จึงเรียนมาเพื่อโปรดสั่งการและประชาสัมพันธ์ให้ทุกหน่วยงานปฏิบัติตามมาตรการอย่างเคร่งครัดต่อไปด้วย จะเป็นพระคุณ

ขอแสดงความนับถือ

(นายพลวรรธน์ วิทูรกลชิต)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
ปฏิบัติราชการแทน ปลัดกระทรวงสาธารณสุข

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กลุ่มคอมพิวเตอร์และเครือข่าย
โทร ๐ ๒๕๙๐ ๑๑๖๙
โทรสาร ๐ ๒๕๙๐ ๑๒๑๕
https://ict.moph.go.th

แนวทางปฏิบัติตามมาตรการป้องกัน Ransomware ชื่อ WannaCry

เนื่องด้วยการระบาดของ Ransomware ชื่อ WannaCry มีการพัฒนาไปในทิศทางที่น่าเป็นห่วง ณ ปัจจุบัน (15/5/60) พบว่า WannaCry ได้พัฒนาเป็นเวอร์ชั่น 2.0 มีความสามารถมากขึ้นกว่าเดิม อีกทั้งยังไม่สามารถบอกได้ว่าจะหยุดพัฒนาเมื่อไร จึงมีความกังวลเกี่ยวกับเครื่องมือแพทย์ที่ใช้กันอยู่ในปัจจุบัน ซึ่งบางเครื่องอาจจะใช้ระบบปฏิบัติการ Windows และอาจลืมดำเนินการ Update โปรแกรมเพื่อป้องกันการโจมตีจากมัลแวร์ต่าง ๆ ดังนั้น การป้องกันจึงเป็นทางเลือกที่ดีที่สุด

แนวทางปฏิบัติ

1. IDENTIFY คอมพิวเตอร์ *ทุกเครื่อง* โดยแยกเป็นกลุ่ม ตามระดับผลกระทบหากถูกโจมตีจากมัลแวร์ (ระบุผู้รับผิดชอบเครื่องแต่ละเครื่อง เช่น หน่วยงาน, ส่วนกลาง, ข้อมูลติดต่อ Vendor)

<u>กลุ่มตามผลกระทบ</u>

A+ : สำคัญต่อชีวิตคนไข้ และ Operation ที่มีการต่อเชื่อมกับระบบ Network

A : ระบบที่เกี่ยวข้องกับการเก็บข้อมูลผู้ป่วย ที่มีการต่อเชื่อมกับระบบ Network

B : ระบบที่เชื่อมต่อกับ HIS ของโรงพยาบาล ที่มีการต่อเชื่อมกับระบบ Network

C : ระบบที่ไม่ได้ต่อเชื่อมกับ HIS ของโรงพยาบาล ที่มีการต่อเชื่อมกับระบบ Network เช่น ระบบสำนักงาน (Back Office)

D : ไม่มีการต่อเชื่อมกับระบบ Network (Stand Alone)

<u>ประเภทบริการ</u>

M : Medical Equipments

L : Laboratory Equipments

U : Utility Equipments (ไฟฟ้า แอร์ ลิฟต์ CCTV)

P : Personal Computer (PC) ทั่วไป

M : Mobile Device

2. วางแผนการจัดการ การตรวจสอบเครื่องแต่ละกลุ่ม และดำเนินการป้องกัน

3. Backup ข้อมูลที่สำคัญออกจากเครื่อง ไว้ใน External Harddisk (ที่ไม่ต่อเชื่อมกับระบบ Network เพื่อป้องกันการถูกเข้ารหัสไฟล์ข้อมูล)

4. สื่อสาร ให้ความรู้เกี่ยวกับการป้องกัน/การลดความเสี่ยงแก่ผู้ใช้งาน (Users) มิให้เป็นพาหะนำมัลแวร์เรียกค่าไถ่ (Ransomware WannaCry) และมัลแวร์อื่น ๆ เข้าสู่เครือข่าย เช่น ไม่เปิดอีเมล์ที่ไม่รู้จัก ไม่คลิกเปิดหรือ Download ไฟล์แนบที่ไม่ระบุแหล่งที่มาที่รู้จัก รวมถึงไฟล์น่าสงสัยอื่น ๆ <u>ห้าม</u>ทดลองเปิดไฟล์ที่อาจเป็นไวรัสหรือมัลแวร์โดยเด็ดขาด

5. จัดทีมเพื่อดำเนินการป้องกัน (ติดตั้ง/Update Patch Windows) และสื่อสารให้ความรู้กับผู้ใช้ และให้มีผู้จัดการ กำกับ และ ติดตามสถานะอย่างใกล้ชิด

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงสาธารณสุขได้ตลอดเวลา
ict-moph@health.moph.go.th