ด่วนที่สุด

ที่ สธ ๐๒๐๒/ว ๑๒๘๓๕

สำนักงานปลัดกระทรวงสาธารณสุข
ถนนติวานนท์ จังหวัดนนทบุรี ๑๑๐๐๐

๑๙ พฤษภาคม ๒๕๖๐

เรื่อง ข้อสั่งการการป้องกันมัลแวร์และไวรัสคอมพิวเตอร์

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

ตามที่มีการแพร่กระจายของมัลแวร์เรียกค่าไถ่ “WannaCry” โจมตีเครื่องคอมพิวเตอร์ทั่วโลก ส่งผลกระทบให้ธุรกิจและบริการ ร่วมถึงทำให้สถานพยาบาลหลายแห่งต้องหยุดบริการ เกิดความเสี่ยงต่อผู้รับบริการอย่างมาก และต้องสูญเสียเงินจำนวนมากเพื่อจ่ายเป็นค่าไถ่คืนข้อมูลสำคัญ ซึ่งรัฐบาลได้กระตุ้นให้ทุกภาคส่วนตระหนักในการป้องกันอย่างเคร่งครัด นั้น

ในการนี้ เพื่อให้หน่วยงานในสังกัดกระทรวงสาธารณสุขและเจ้าหน้าที่ทุกคนให้ความสำคัญในการปฏิบัติตามแนวทางการป้องกัน Ransomware ชื่อ WannaCry รวมทั้งมัลแวร์และไวรัสคอมพิวเตอร์อื่น ๆ อย่างเคร่งครัด สำนักงานปลัดกระทรวงสาธารณสุข จึงมีข้อสั่งการให้หน่วยงานปฏิบัติ ดังนี้

๑. ทบทวนมาตรการการรักษาความปลอดภัยสารสนเทศของหน่วยงานที่ดำเนินการตามประกาศกระทรวงสาธารณสุข ณ วันที่ ๗ มกราคม พ.ศ. ๒๕๕๖ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และปรับปรุงให้มีความทันสมัย ครอบคลุมการพิสูจน์ยืนยันตัวตนในการเข้าถึงระบบงาน การแยกเครือข่ายเฉพาะอุปกรณ์ทางการแพทย์ การตรวจสอบติดตาม การป้องกัน การตอบสนองต่อเหตุการณ์ การสำรองข้อมูลไว้นอกเครือข่าย และการกู้คืนระบบข้อมูลสำคัญ (Download ประกาศได้ที่ https://ict.moph.go.th/th/extension/196)

๒. ประกาศมาตรการการรักษาความปลอดภัยสารสนเทศของหน่วยงาน ให้เจ้าหน้าที่ทุกคนภายในหน่วยงานทราบ ทำความเข้าใจ และถือปฏิบัติอย่างเคร่งครัด

๓. จัดตั้งทีมเฝ้าระวังการโจมตีระบบเครือข่าย ทั้งจากเครือข่ายภายนอก (Internet) และภายในเครือข่ายของหน่วยงาน (Intranet)

๔. จัดตั้งทีมตรวจสอบและให้ความช่วยเหลือเจ้าหน้าที่ในการ Update Patch ของ Windows ทั้งเครื่องลูกข่าย อุปกรณ์การแพทย์และห้องปฏิบัติการ รวมถึงอุปกรณ์อื่น ๆ ที่อาจมีความเสี่ยงโดนโจมตี และทำการปิด Service SMBv1 ดังรายละเอียดที่ https://www.thaicert.or.th/downloads/downloads.html และ https://ict.moph.go.th

ทั้งนี้ ...

ทั้งนี้ หากหน่วยงานใดต้องการความช่วยเหลือ หรือขอคำปรึกษา สามารถติดต่อได้ที่ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข โทร ๐ ๒๕๙๐ ๑๑๖๙, ๑๒๐๑, ๐๘ ๗๐๒๗ ๖๖๖๓ email : ict-moph@health.moph.go.th และผ่านช่องทาง Social Network ได้ที่ Line : @ict-moph-ops01 และ https://www.facebook.com/MophICT/ ตลอด ๒๔ ชั่วโมง

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติดำเนินการโดยเคร่งครัด จะเป็นพระคุณ

ขอแสดงความนับถือ

(นายโสภณ เมฆธน)
ปลัดกระทรวงสาธารณสุข

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กลุ่มคอมพิวเตอร์และเครือข่าย
โทร ๐ ๒๕๙๐ ๑๑๖๙
โทรสาร ๐ ๒๕๙๐ ๑๒๑๕

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

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

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