



ที่ ลป ๐๐๑๙.๔/ว ๑๓๕๖๘

ศาลากลางจังหวัดลำปาง
กม.๕ ถนนชริราษฎร์ดำเนิน
ตำบลพระบาท ลป ๕๒๐๐๐

๑ มิถุนายน ๒๕๖๐

เรื่อง การป้องกันและเฝ้าระวังภัยมัลแวร์เรียกค่าไถ่ Wannacry แพร่กระจายผ่านช่องโหว่ของวินโดวส์
เรียน นายอำเภอทุกอำเภอ

สิ่งที่ส่งมาด้วย สำเนาหนังสือสำนักงานปลัดกระทรวงมหาดไทย ด่วนที่สุด ที่ มท ๐๒๑๐.๓/ว.๒๖๓๕
ลงวันที่ ๑๖ พฤษภาคม ๒๕๖๐

ด้วยกรมการพัฒนาชุมชน ได้แจ้งแนวทางการป้องกันและเฝ้าระวังภัยมัลแวร์เรียกค่าไถ่ Wannacry แพร่กระจายผ่านช่องโหว่ของวินโดวส์ จากสำนักงานปลัดกระทรวงมหาดไทย ที่แจ้งให้หน่วยงานในสังกัดได้ใช้เป็นแนวทางปฏิบัติในการป้องกันภัยมัลแวร์เรียกค่าไถ่ Wannacry ให้มีประสิทธิภาพ

เพื่อเป็นการป้องกันและเฝ้าระวังภัยมัลแวร์เรียกค่าไถ่ Wannacry แพร่กระจายผ่านช่องโหว่ของวินโดวส์ จึงขอให้แจ้งพัฒนาการอำเภอ ได้กำกับดูแลให้เจ้าหน้าที่ทุกคนในสังกัดสำนักงานพัฒนาชุมชนอำเภอ ดำเนินการต่อไปนี้ โดยเคร่งครัด

๑. ไม่เปิดเอกสารแนบอีเมลโดยไม่จำเป็น หากจำเป็นต้องเปิดเอกสารแนบอีเมลควรตรวจสอบกับผู้ส่งก่อนว่าได้ส่งอีเมลฉบับนั้นมาจริง
๒. เพื่อลดความเสี่ยงของ Malware ที่เครื่องคอมพิวเตอร์ควรทำการ Update patch เดียวกัน เพื่อลดโอกาสที่ผู้ใช้งานจะนำ Malware นี้เข้ามาระบาดขององค์กร
๓. ควรสำรองข้อมูลบนเครื่องคอมพิวเตอร์ที่ใช้งานอย่างสม่ำเสมอ และหากเป็นไปได้ให้เก็บข้อมูลที่ทำการสำรองไว้ในอุปกรณ์ที่ไม่มีการเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายอื่น ๆ
๔. ติดตั้งโปรแกรมป้องกันไวรัสฯ ให้กับเครื่องคอมพิวเตอร์ของหน่วยงานทุกเครื่องจากแผ่นดีดี ติดตั้งโปรแกรมป้องกันไวรัสฯ โดยศึกษาคู่มือการติดตั้งและการใช้งานโปรแกรมป้องกันไวรัส Eset Endpoint เวอร์ชัน 6.4.2014.0
๕. เปิดเครื่องคอมพิวเตอร์เพื่อให้โปรแกรมป้องกันไวรัสอัปเดต (update) และระบบจะทำการสแกนไวรัสอัตโนมัติทุกวันเวลา ๑๒.๐๐ น.

จึงเรียนมาเพื่อพิจารณาดำเนินการ

ขอแสดงความนับถือ

นางศลิษา ม่วงใหม่

นักวิชาการพัฒนาชุมชนชำนาญการพิเศษ รักษาการแทน

พัฒนาการจังหวัด ปฏิบัติราชการแทน

ผู้ว่าราชการจังหวัดลำปาง

สำนักงานพัฒนาชุมชนจังหวัดลำปาง
โทร. โทรสาร ๐ ๕๔๒๖ ๕๐๕๕



กรมการพัฒนาชุมชน : เศรษฐกิจฐานรากมั่นคงและชุมชนพึ่งตนเองได้ ภายในปี ๒๕๖๔



ด่วนที่สุด

บันทึกข้อความ

กรมการพัฒนาระบบ
เลขที่ 234
วันที่ 17 พ.ค. 2560
เวลา 14.40 น.

ส่วนราชการ สำนักงานปลัดกระทรวงมหาดไทย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โทร ๐๒ ๒๒๓ ๒๐๐๐
 ที่ มท ๐๒๑๐.๓/ว ๒๖๓๕ วันที่ ๑๖ พฤษภาคม ๒๕๖๐ ศูนย์สารสนเทศฯ

เรื่อง การป้องกันและเผื่อระวังภัยมัลแวร์เรียกค่าไถ่ WannaCry แพร่กระจายผ่านช่องโหว่ของวินโดวส์.ศ. 2560

เรียน หัวหน้าส่วนราชการระดับกรม หัวหน้าหน่วยงานรัฐวิสาหกิจในสังกัดกระทรวงมหาดไทย
 หน่วยงานในสังกัดสำนักงานปลัดกระทรวงมหาดไทย และสำนักงานรัฐมนตรี กระทรวงมหาดไทย

ตามที่มีข่าวสารกระจายในวงกว้างถึงเรื่องภัยจากการติดมัลแวร์เรียกค่าไถ่ (Ransomware) สายพันธุ์ชื่อ WannaCry โดยมีมัลแวร์ดังกล่าว มีจุดประสงค์หลักเพื่อเข้ารหัสลับข้อมูลไฟล์เอกสารและไฟล์สำคัญทั้งหมด รวมถึงมีความสามารถในการกระจายตัวเองจากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อื่น ๆ ในเครือข่ายได้โดยอัตโนมัติ ผ่านช่องโหว่ของวินโดวส์ที่เกี่ยวกับการบริหารแชร์ไฟล์ผ่านเครือข่าย (Server Message Block : SMB) ที่มีการเปิดให้บริการ นำมาเรียกค่าไถ่ หากไม่จ่ายเงินตามที่เรียกจะไม่สามารถเปิดไฟล์ได้นั้น

ดังนั้น เพื่อเป็นการป้องกันและเผื่อระวังภัยมัลแวร์ดังกล่าว สำนักงานปลัดกระทรวงมหาดไทย ได้จัดทำแนวทางในการป้องกัน ดังนี้

(๑) แนวทางการป้องกันการติด Ransomware สำหรับผู้ดูแลระบบ

(๑.๑) ปรับปรุงระบบปฏิบัติการ Microsoft Windows ให้เป็นปัจจุบันเสมอ เพื่อป้องกันการใช้ช่องโหว่ของระบบซึ่งเป็นช่องทางให้คอมพิวเตอร์ติด Ransomware หากเป็นไปได้ควรหยุดใช้งานระบบปฏิบัติการ Windows XP, Windows Server ๒๐๐๓ และ Windows Vista เนื่องจากสิ้นสุดระยะเวลาสนับสนุนด้านความมั่นคงปลอดภัยแล้ว หากยังจำเป็นต้องใช้งานไม่ควรใช้กับระบบที่มีข้อมูลสำคัญ

(๑.๒) กรณีเครื่องคอมพิวเตอร์แม่ข่าย (Server) หรือระบบที่สำคัญ และไม่สามารถ Patch ได้ในทันที ควรทำการ Disable SMBv๑ หากไม่ได้ทำการใช้งาน

(๑.๓) ปิด Port Remote การเข้าถึงผ่าน RDP (Remote Desktop Protocol) และ SMB จาก Internet ของระบบที่มีความเสี่ยง

(๑.๔) ติดตั้งแอนติไวรัสและอัปเดตฐานข้อมูลอย่างสม่ำเสมอ ปัจจุบันแอนติไวรัสส่วนใหญ่ (รวมถึง Windows Defender ของ Microsoft) สามารถตรวจจับมัลแวร์ WannaCry สายพันธุ์ที่กำลังมีการแพร่ระบาดได้แล้ว

(๒) แนวทางการป้องกันการติด Ransomware สำหรับผู้ใช้งาน

(๒.๑) ไม่เปิดเอกสารแนบอีเมลโดยไม่จำเป็น หากจำเป็นต้องเปิดเอกสารแนบอีเมลควรตรวจสอบกับผู้ส่งก่อนว่าได้ส่งอีเมลฉบับนั้นมาจริง

(๒.๒) เพื่อลดความเสี่ยงของ Malware ที่เครื่องคอมพิวเตอร์ควรทำการ Update Patch เดียวกัน เพื่อลดโอกาสที่ผู้ใช้งานจะนำ mailware นี้เข้ามาระบาดของในองค์กร

(๒.๓) ควรสำรองข้อมูลบนเครื่องคอมพิวเตอร์ที่ใช้งานอย่างสม่ำเสมอ และหากเป็นไปได้ ให้เก็บข้อมูลที่ทำการสำรองไว้ในอุปกรณ์ที่ไม่มีการเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายอื่น ๆ

จึงเรียนมาเพื่อพิจารณาดำเนินการต่อไป

(นายณัฐพงศ์ ศิริชนะ)
 รองปลัดกระทรวงมหาดไทย ปฏิบัติราชการแทน
 ปลัดกระทรวงมหาดไทย