ที่ สค ๐๐๑๗.๒/ว ๑๓๖๗

ศาลากลางจังหวัดสมุทรสาคร
ถนนเศรษฐกิจ ๑ สค ๗๔๐๐๐

๑๙ พฤษภาคม ๒๕๖๐

เรื่อง การป้องกันและเฝ้าระวังภัยมัลแวร์เรียกค่าไถ่ WannaCry แพร่กระจายผ่านช่องโหว่ของวินโดวส์

เรียน หัวหน้าส่วนราชการ หัวหน้าหน่วยงานรัฐวิสาหกิจ นายอำเภอทุกอำเภอ นายกองค์การบริหารส่วนจังหวัดสมุทรสาคร นายกเทศมนตรีนครสมุทรสาคร นายกเทศมนตรีนครอ้อมน้อย และนายกเทศมนตรีเมืองกระทุ่มแบน

สิ่งที่ส่งมาด้วย สำเนาหนังสือกระทรวงมหาดไทย ด่วนที่สุด ที่ มท ๐๒๑๐.๓/ว ๒๖๓๔ ลงวันที่ ๑๖ พฤษภาคม ๒๕๖๐

ด้วยกระทรวงมหาดไทยแจ้งว่าตามที่มีข่าวสารกระจายในวงกว้างถึงเรื่องภัยจากการติดมัลแวร์เรียกค่าไถ่ (Ransomware) สายพันธุ์ชื่อ WannaCry โดยมัลแวร์ดังกล่าว มีจุดประสงค์หลักเพื่อเข้ารหัสลับข้อมูลไฟล์เอกสารและไฟล์สำคัญทั้งหมด รวมถึงมีความสามารถในการกระจายตัวเองจากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อื่น ๆ ในเครือข่ายได้โดยอัตโนมัติ ผ่านช่องโหว่ของวินโดว์ที่เกี่ยวข้องกับการบริหารแชร์ไฟล์ผ่านเครือข่าย (Server Message Block : SMB) ที่มีการเปิดให้บริการ นำมาเรียกค่าไถ่ หากไม่จ่ายเงินตามที่เรียกจะไม่สามารถเปิดไฟล์ได้

เพื่อเป็นการป้องกันและเฝ้าระวังภัยมัลแวร์ดังกล่าว จังหวัดสมุทรสาครจึงขอให้หน่วยงานดำเนินการตามแนวทางป้องกันของกระทรวงมหาดไทย ดังนี้

๑. แนวทางการป้องกันการติด Ransomware สำหรับผู้ดูแลระบบ

๑.๑ ปรับปรุงระบบปฏิบัติการ Microsoft Windows ให้เป็นปัจจุบันเสมอ เพื่อป้องกันการใช้ช่องโหว่ของระบบซึ่งเป็นช่องทางให้คอมพิวเตอร์ติด Ransomware หากเป็นไปได้ควรหยุดการใช้งานระบบปฏิบัติการ 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 เดียวกันเพื่อลดโอกาสที่ผู้ใช้งานจะนำ Malware นี้เข้ามาระบาดในองค์กร

๒.๓ ควรสำรอง...

๒.๓ ควรสำรองข้อมูลบนเครื่องคอมพิวเตอร์ที่ใช้งานอย่างสม่ำเสมอ และหากเป็นไปได้ให้เก็บข้อมูลที่ทำการสำรองไว้ในอุปกรณ์ที่ไม่มีการเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายอื่น ๆ

จึงเรียนมาเพื่อพิจารณาดำเนินการ สำหรับอำเภอขอให้แจ้งองค์กรปกครองส่วนท้องถิ่นในพื้นที่ดำเนินการด้วย

ขอแสดงความนับถือ

(นายประภัสสร์ มาลากาญจน์)
ผู้ว่าราชการจังหวัดสมุทรสาคร

สำนักงานจังหวัด
กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด
โทร. ๐ ๓๔๔๒ ๕๐๗๕
ไปรษณีย์อิเล็กทรอนิกส์ : strategy.skn@gmail.com

ด่วนที่สุด

ที่ มท ๐๒๑๐.๓/ว๒๖๓๔

สำนักงานปลัดกระทรวงมหาดไทย
ถนนอัษฎางค์ กทม. ๑๐๒๐๐

๑๖ พฤษภาคม ๒๕๖๐

เรื่อง การป้องกันและเฝ้าระวังภัยมัลแวร์เรียกค่าไถ่ WannaCry แพร่กระจายผ่านช่องโหว่ของวินโดวส์

เรียน ผู้ว่าราชการจังหวัดทุกจังหวัด

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

ดังนั้น เพื่อเป็นการป้องกันและเฝ้าระวังภัยมัลแวร์ดังกล่าว สำนักงานปลัดกระทรวงมหาดไทย ได้จัดทำแนวทางในการป้องกัน ดังนี้

(๑) แนวทางการป้องการการติด Ransomware สำหรับผู้ดูแลระบบ

(๑.๑) ปรับปรุงระบบปฏิบัติการ Microsoft Windows ให้เป็นปัจจุบันเสมอ เพื่อป้องกันการใช้ช่องโหว่ของระบบซึ่งเป็นช่องทางให้คอมพิวเตอร์ติด Ransomware หากเป็นได้ได้ควรหยุดใช้งานระบบปฏิบัติการ 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) ติดตั้งแอนตี้ไวรัสและอัปเดตฐานข้อมูลอย่างสม่ำเสมอ ปัจจุบันแอนตี้ไวรัสส่วนใหญ่ (รวมถึง Windows Defender ของ Microsoft) สามารถตรวจจับมัลแวร์ WannaCry สายพันธุ์ที่กำลังมีการแพร่ระบาดได้แล้ว

(๒) แนวทางการป้องการการติด Ransomware สำหรับผู้ใช้งาน

(๒.๑) ไม่เปิดเอกสารแนบอีเมลโดยไม่จำเป็น หากจำเป็นต้องเปิดเอกสารแนบอีเมลควรตรวจสอบกับผู้ส่งก่อนว่าได้ส่งอีเมลฉบับนั้นมาจริง

(๒.๒) เพื่อลดความเสี่ยงของ Malware ที่เครื่องคอมพิวเตอร์ควรทำการ Update Patch เตียวกัน เพื่อลดโอกาสที่ผู้ใช้งานจะนำ mailware นี้เข้ามาระบาดในองค์กร

/ (๒.๓) ควรสำรอง...

(๒.๓) ควรสำรองข้อมูลบนเครื่องคอมพิวเตอร์ที่ใช้งานอย่างสม่ำเสมอ และหากเป็นไปได้ให้เก็บข้อมูลที่ทำการสำรองไว้ในอุปกรณ์ที่ไม่มีการเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายอื่นๆ

จึงเรียนมาเพื่อพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายณัฐพงศ์ ศิริชนะ)
รองปลัดกระทรวงมหาดไทย ปฏิบัติราชการแทน
ปลัดกระทรวงมหาดไทย

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทร ๐-๒๒๒๖-๐๕๐๕ โทร (มท) ๕๐๔๗๖
โทรสาร ๐-๒๒๒๓-๕๒๔๑ โทร (มท) ๕๐๖๖๖