ศสช.

ด่วนที่สุด

บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ กพช. โทร. ๐-๒๖๑๘-๒๓๒๓ ต่อ ๑๐๑๕

ที่ นร ๐๒๐๖.๐๓/ ๔๔๗ **วันที่** ๑๗ พฤษภาคม ๒๕๖๐

เรื่อง มาตรการระมัดระวังการติดมัลแวร์ Wanna Crypt ภายในองค์กร

เรียน อปส. ผ่าน รปส.(๓)

ด้วย ขณะนี้มีมัลแวร์เรียกค่าไถ่ชื่อ Wanna Crypt (Wanna Decryptor ๒.๐) แพร่ระบาดไปยังเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Microsoft ทั่วโลก โดยผู้ใช้งานคอมพิวเตอร์อาจดาวน์โหลดมัลแวร์โดยไม่รู้ตัว จากการเปิดไฟล์เอกสารที่แนบมากับ E-mail ซึ่งเมื่อมัลแวร์ดังกล่าวทำงานจะทำให้ผู้ใช้งานไม่สามารถเปิดไฟล์เอกสารต่าง ๆ ภายในเครื่องเพื่อใช้งานได้ และต้องจ่ายเงินค่าไถ่เพื่อปลดล็อคเอกสาร ตามที่มีการเผยแพร่ข่าวโดยทั่วไป

ในการนี้ ศสช. ซึ่งเป็นหน่วยงานหลักในการบริหารจัดการระบบสารสนเทศภายใน กปส. ขอเสนอว่า ควรมีมาตรการขั้นสูงสุด เพื่อให้ทุกหน่วยงานที่ใช้งานและปฏิบัติราชการประจำวันด้วยเครื่องคอมพิวเตอร์ผ่านระบบอินเทอร์เน็ตและแบบใช้งานส่วนบุคคลให้เพิ่มความระมัดระวัง เพื่อป้องกันการก่อให้เกิดผลเสียหายอันจะตามมาในภายหลัง จึงเห็นควรให้ดำเนินการในแนวทางเดียวกัน ดังนี้

๑. สำหรับหน่วยงานที่มีหรือรับผิดชอบระบบการให้บริหารหลัก (เว็บไซต์, เครื่องคอมพิวเตอร์แม่ข่าย, ระบบเว็บเซอร์วิส และอุปกรณ์ Firewall) ให้ดำเนินการในส่วนที่เกี่ยวข้อง ตามเอกสารแนบ

๒. สำหรับผู้ใช้งาน มีข้อระมัดระวังในการใช้งาน ดังนี้

๒.๑ Update patch ของระบบปฏิบัติการ Microsoft Windows ของเครื่องคอมพิวเตอร์พร้อมรีสตาร์ทให้มีการอัพเดตมีผลโดยสมบูรณ์

๒.๒ ควรคิดก่อนคลิ๊ก หลีกเลี่ยงการเปิดไฟล์แนบใน E-mail (E-mail attachment) หรือ Link บนเว็บไซต์ที่ไม่แน่ใจว่าปลอดภัยหรือไม่

๒.๓ ทำการสำรองข้อมูล และเก็บไว้ในที่ปลอดภัยเสมอ และเก็บไว้ Offline โดยไม่เชื่อมต่อกับเครื่องขณะใช้งาน

๒.๔ ตระหนักถึงการใช้ระบบสารสนเทศ (IT) โดยอยู่บนพื้นฐานของความปลอดภัยอยู่เสมอ

๒.๕ ในกรณีที่มีหน้าจอ ransomware หรือพบอาการผิดปกติให้รีบถอดสาย LAN ออก และถ่ายภาพหรือ Screenshot ไว้ แล้วรีบแจ้งเจ้าหน้าที่ผู้ดูและระบบโดยทันที จึงขอให้ผู้ที่ใช้เครื่องคอมพิวเตอร์ และผู้มีหน้าที่ดูแลระบบสารสนเทศของหน่วยงานในกรมประชาสัมพันธ์รับทราบ พร้อมทั้ง เพิ่มความระมัดระวังและปฏิบัติตามเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาเห็นชอบให้ใช้มาตรการป้องกันดังกล่าว ทั้งนี้ ศสช. จะได้เวียนแจ้งให้หน่วยงานต่าง ๆ ได้ถือปฏิบัติต่อไป

(นายนรกิจ ศรัทธา)
ผอ.ศสช.

- เห็นชอบ
- ดำเนินการตามเสนอ

(นางสาวศุภพร สาครบุตร)
ป.อปส.
๑๕ พ.ค.๖๐

ด่วนที่สุด

เรียน ผอ.สำนัก/กอง และหัวหน้าหน่วยงานต่างๆ

เพื่อโปรดทราบ และกรุณาแจ้งเวียนให้บุคลากรในหน่วยงานทราบ และถือปฏิบัติ

(นายนรกิจ ศรัทธา)
ผอ.ศสช.
๑๘ พ.ค. ๒๕๖๐

รปส. (นางสาวศุภพร สาครบุตร) ๑๘/๕/๖๐

มาตรการป้องกันมัลแวร์ WannaCrypt

1. ปิดการใช้งาน SMBv1 หากไม่จำเป็น โดยทำการบล็อก และเฝ้าระวังการเชื่อมต่อบริการ SMB (Port 137, 138, 139, 445) จากเครือข่ายภายนอก

2. ในกรณีที่จำเป็นต้องมีการใช้ SMBv1 จากภายใน ให้ติดตั้ง Security Update MS17-010 จาก Microsoft (https://technet.microsoft.com/en-us/library/security/ms17-010.aspx) เพื่อแก้ไขช่องโหว่ และอนุญาตเท่าที่จำเป็นเท่านั้น

3. หากมีการแชร์ข้อมูลร่วมกันผ่านระบบเครือข่าย ให้ตรวจสอบสิทธิในการเข้าถึงข้อมูลแต่ละส่วน และกำหนดสิทธิ์ให้ผู้ใช้มีสิทธิ์อ่านหรือแก้ไขเฉพาะไฟล์ที่มีความจำเป็นต้องใช้สิทธิเหล่านั้น

4. อัพเดตระบบปฏิบัติการให้เป็นเวอร์ชันล่าสุดอยู่เสมอ หากเป็นได้ได้ควรหยุดใช้งานระบบปฏิบัติการ Windows XP, Windows Server 2003 และ Windows Vista เนื่องจากสิ้นสุดระยะเวลาสนับสนุนด้านความมั่นคงปลอดภัยแล้ว หากยังจำเป็นต้องใช้งานไม่ควรใช้กับระบบที่มีข้อมูลสำคัญ

5. ติดตั้งแอนตี้ไวรัสและอัปเดตฐานข้อมูลอย่างสม่ำเสมอ

6. สำรองข้อมูลบนเครื่องคอมพิวเตอร์ที่ใช้งานอย่างสม่ำเสมอ และหากเป็นไปได้ให้เก็บข้อมูลที่ทำการสำรองไว้ในอุปกรณ์ที่ไม่มีการเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายอื่นๆ

7. ตั้งค่า Firewall เพื่อบล็อกการเชื่อมต่อกับไอพีแอดเดรสปลายทาง ดังนี้

- 213.61.66.116, 171.25.193.9, 163.172.35.247, 128.31.0.39, 185.97.32.18, 178.62.173.203, 136.243.176.148, 217.172.190.251, 94.23.173.93, 50.7.151.47, 83.162.202.182, 163.172.185.132, 163.172.153.12, 62.138.7.231

8. ไม่ควรเปิดอ่าน อีเมลล์และ ไฟล์แนบจากอีเมล์ที่ไม่รู้จักโดยเฉพาะซิปไฟล์ เพราะแค่เปิดซิปไฟล์ สคลิป ransomeware จะทำงานทันที

*** ปัจจุบันมัลแวร์ WannaCrypt ที่แพร่กระจายผ่านช่องโหว่ SMBv1 เป็นเวอร์ชัน 2.0 ซึ่งในขณะนี้ยังไม่มีวิธีการแก้ไขให้สามารถกลับมาใช้งานไฟล์ได้

มีข้อสงสัยเพิ่มเติม สอบถามได้ที่

นายจิระศักดิ์ โตรัตน์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ โทร 02-6182323 ต่อ 1213
e-mail :jirasak_t@prd.go.th กลุ่มพัฒนาเทคนิคและเชื่อมโยงเครือข่าย ศสช. กปส.
