แนวทางการป้องกัน และการจัดการเมื่อติดมัลแวร์เรียกค่าไถ่ (Ransomware) ชื่อ WannaCry

การบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบคอมพิวเตอร์

๑. ให้สำรองข้อมูล (Backup Data) ในเครื่องคอมพิวเตอร์แม่ข่าย (Server) ตามแผนปฏิบัติการอย่างสม่ำเสมอ และตรวจสอบการกู้คืนระบบ (Restore)

๒. ปรับปรุงช่องโหว่หรือจุดอ่อนของระบบปฏิบัติการ Microsoft Windows (Update Patch) และปรับปรุงโปรแกรมพื้นฐานที่ฝังตัวอยู่ในฮาร์ดแวร์ (Firmware) ให้เป็นปัจจุบัน และในกรณีระบบหรือเครื่องคอมพิวเตอร์แม่ข่ายที่มีการจ้างบำรุงรักษา จะต้องมีการตรวจสอบให้บริษัทผู้รับจ้างทำการ Update Patch ระบบปฏิบัติการ และปรับปรุง Firmware ของระบบให้เป็นปัจจุบัน **ทั้งนี้** ให้มีการทดสอบการทำงานของระบบที่เกี่ยวข้องทุกฟังก์ชัน ถึงผลกระทบในการดำเนินงาน และในกรณีไม่สามารถ Patch ได้ในทันที ควรทำการ Disable: SMBv1 (Server Message Block) หากไม่ได้ใช้งาน

๓. ปิดการใช้งาน SMBv1 (Server Message Block) ของระบบปฏิบัติการ Microsoft Windows เพื่อป้องกันช่องโหว่ของ SMB เวอร์ชั่น ๑ ซึ่งเป็นช่องทางในการแพร่กระจายตัวเองของ Ransomware จากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อื่น ๆ ในเครือข่ายได้โดยอัตโนมัติ ในกรณีที่ผู้ใช้งานไม่อัพเดตระบบปฏิบัติการวินโดวส์ซึ่งจะมีความเสี่ยงที่จะติดมัลแวร์ดังกล่าว

การบริหารจัดการเครื่องคอมพิวเตอร์ลูกข่าย และระบบคอมพิวเตอร์ของส่วนราชการในสังกัดกรมที่ดิน

๑. แนวทางการป้องกันการติดมัลแวร์เรียกค่าไถ่

๑.๑ ให้สำรองไฟล์ข้อมูล (Copy file) ในเครื่องคอมพิวเตอร์เป็นประจำทุกวันอย่างสม่ำเสมอ โดยควรเก็บข้อมูลที่ทำการสำรองไว้ในอุปกรณ์อื่นใดภายนอกเครื่องคอมพิวเตอร์ หรือจัดเก็บไว้หลายแห่ง และไม่ควรคลิกลิงก์หรือเปิดไฟล์ที่แนบมาพร้อมกับอีเมลที่น่าสงสัย หากไม่มั่นใจว่าเป็นอีเมลที่น่าเชื่อถือหรือไม่รู้จักผู้ส่งอีเมล ให้ลบอีเมลนั้นทิ้งไป และควรดาวน์โหลดซอฟต์แวร์จากแหล่งที่น่าเชื่อถือเท่านั้น

๑.๒ ปรับปรุงช่องโหว่หรือจุดอ่อนของระบบปฏิบัติการ Microsoft Windows (Patch)

๑.๓ ปิดการใช้งาน SMBv1 (Server Message Block) ของระบบปฏิบัติการ Microsoft Windows (หากไม่ได้ใช้งาน) เพื่อป้องกันช่องโหว่ของ SMB เวอร์ชั่น ๑ ที่เป็นช่องทางในการแพร่กระจายตัวเองของ Ransomware จากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อื่น ๆ ในเครือข่ายได้โดยอัตโนมัติ ในกรณีที่ผู้ใช้งานไม่อัพเดตระบบปฏิบัติการวินโดวส์ซึ่งจะมีความเสี่ยงที่จะติดมัลแวร์ดังกล่าว

๒. วิธีการจัดการเมื่อติดมัลแวร์เรียกค่าไถ่

๒.๑ ให้ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อกับระบบเครือข่ายสื่อสารของกรมที่ดินและเครือข่ายอินเทอร์เน็ตในทันที โดยการถอดสาย LAN ออก

๒.๒ ทำการ Format เครื่องคอมพิวเตอร์ทุกไดรฟ์ (Drive) เพื่อล้างข้อมูลทั้งหมด และติดตั้งระบบปฏิบัติการใหม่โดยใช้แผ่น CD หรือ DVD เท่านั้น