ด่วนที่สุด

บันทึกข้อความ

ส่วนราชการ สำนักเทคโนโลยีสารสนเทศ โทรศัพท์ ๐-๒๙๘๔-๐๘๑๙ โทรสาร ๐-๒๕๐๓-๓๖๗๙
ที่ มท ๐๕๑๓.๒ /๑๗๐๖ **วันที่** ๑๘ พฤษภาคม ๒๕๖๐
เรื่อง แนวทางการป้องกัน และการแก้ไขเมื่อติดมัลแวร์เรียกค่าไถ่ (Ransomware) ชื่อ WannaCry

เรียน อธิบดีกรมที่ดิน

๑. เรื่องเดิม

กรมที่ดินได้ให้ความสำคัญในการดำเนินการตามกฎหมายเทคโนโลยีสารสนเทศที่เกี่ยวข้อง และมีมาตรการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร พร้อมสร้างความตระหนักรู้ (Awareness) ให้กับเจ้าหน้าที่ของหน่วยงานในสังกัด ดังนี้

๑.๑ จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมที่ดิน เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร และกำชับให้เจ้าหน้าที่นำไปใช้ในการปฏิบัติงานและถือปฏิบัติอย่างเคร่งครัด พร้อมให้ความร่วมมือในการใช้เทคโนโลยีสารสนเทศและเครือข่ายสื่อสารของกรมที่ดินภายใต้กฎหมายเทคโนโลยีสารสนเทศ เพื่อประสิทธิภาพการใช้งานและความมั่นคงปลอดภัยโดยรวม ตามหนังสือกรมที่ดิน ที่ มท ๐๕๑๓.๒/ว ๒๔๑๔ ลงวันที่ ๓๐ มกราคม ๒๕๖๐ ***(เอกสารหมายเลข ๑)*** และบันทึกสำนักเทคโนโลยีสารสนเทศ ที่ มท ๐๕๑๓.๒ /ว ๖๖๑ ลงวันที่ ๙ กุมภาพันธ์ ๒๕๖๐ ***(เอกสารหมายเลข ๒)***

๑.๒ จัดหาระบบรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร พร้อมจัดเจ้าหน้าที่ผู้เชี่ยวชาญตรวจสอบนโยบายและการกำหนดค่าเบื้องต้นของแต่ละอุปกรณ์เพื่อตรวจหาและปรับปรุงช่องโหว่หรือจุดอ่อนของระบบคอมพิวเตอร์อย่างสม่ำเสมอ เป็นระยะ ๆ ตามวิวัฒนาการของการโจมตีในรูปแบบต่าง ๆ เพื่อเป็นการป้องกันผู้ไม่ประสงค์ดีอาศัยช่องโหว่ของซอฟต์แวร์ระบบ เข้าโจมตีหรือขโมยข้อมูลสำคัญในระบบคอมพิวเตอร์ของกรมที่ดิน ซึ่งไม่อาจคาดการณ์วิธีการโจมตีได้ว่าจะมาในรูปแบบใด

๑.๓ จัดหาโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย สำหรับติดตั้งใช้งานในเครื่องคอมพิวเตอร์ของส่วนราชการในสังกัดกรมที่ดินทั้งในส่วนกลาง และสำนักงานที่ดินจังหวัด/สาขา/ส่วนแยก/อำเภอทั่วประเทศ โดยได้ดำเนินการมาอย่างต่อเนื่อง เพื่อป้องกันไวรัสคอมพิวเตอร์ที่อาจจะทำลายฐานข้อมูลสำคัญในเครื่องคอมพิวเตอร์ ***(เอกสารหมายเลข ๓)***

๒. ข้อเท็จจริง

๒.๑ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมที่ดิน ได้กำหนดมาตรฐาน/แนวทางและระเบียบปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ผู้ดูแลระบบ และผู้ใช้งานระบบ ใช้เป็นแนวทางในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันความเสี่ยง ความเสียหาย หรืออันตรายที่อาจเกิดขึ้น และในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่กรมที่ดิน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมที่ดิน ผู้ใช้งานที่เจตนาฝ่าฝืนนโยบายฯ แม้ว่าการฝ่าฝืนนั้นจะกระทำไม่บรรลุผลโดยสมบูรณ์ ให้ถือว่ามีความผิดโดยสมบูรณ์ จะต้องรับโทษตามบทลงโทษที่กำหนด ***(เอกสารหมายเลข ๔)***

๒.๒ ผลจากการ...

๒.๒ ผลจากการตรวจสอบการติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมายทดแทนลิขสิทธิ์ชุดเดิมที่สิ้นสุดระยะเวลาการใช้งานแล้ว ในเครื่องคอมพิวเตอร์ของทางราชการที่เชื่อมต่อกับเครือข่ายสื่อสารกรมที่ดิน พบว่า สำนัก/กองส่วนกลาง และสำนักงานที่ดินทั่วประเทศได้ติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัสคอมพิวเตอร์ไปแล้ว จำนวนรวมทั้งสิ้น ๖,๓๕๓ เครื่อง ทั้งนี้ สำนักเทคโนโลยีสารสนเทศได้ให้เจ้าหน้าที่ที่ไปตรวจติดตามงานโครงการต่าง ๆ ตรวจสอบและกำชับให้เจ้าหน้าที่ของสำนักงานที่ดินให้ความสำคัญในการติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่ได้จัดส่งให้

๒.๓ ด้วยขณะนี้ มีมัลแวร์ (Malware) เรียกค่าไถ่ (Ransomware) ชื่อ WannaCry หรือ Wanna Decryptor 2.0 ระบาดไปยังคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Microsoft Windows ทั่วโลก โดยเมื่อวันที่ ๑๒ พฤษภาคม ๒๕๖๐ พลเอกประยุทธ์ จันทร์โอชา นายกรัฐมนตรี ได้ประกาศเตือนประชาชนให้ระมัดระวังการดาวน์โหลดไฟล์เอกสารจากโลกออนไลน์ ซึ่งผู้ใช้งานอาจจะดาวน์โหลดมัลแวร์ หรือโปรแกรมที่ถูกสร้างขึ้นมาเพื่อสร้างความเสียหายแก่ข้อมูลในระบบคอมพิวเตอร์ได้

๓. ข้อพิจารณา

สำนักเทคโนโลยีสารสนเทศได้จัดประชุมเจ้าหน้าที่ผู้เกี่ยวข้องเพื่อหารือแนวทางในการป้องกันข้อมูลสำคัญในระบบคอมพิวเตอร์ และการบริหารจัดการมัลแวร์เรียกค่าไถ่ (Ransomware) ชื่อ WannaCry เนื่องจากขณะนี้ ยังไม่มีวิธีการแก้ไขปัญหามัลแวร์ดังกล่าว นอกจากการจ่ายเงินเรียกค่าไถ่ข้อมูลเป็น BIT Coin (สกุลเงินดิจิทัล) เพื่อแลกกับรหัสผ่านสำหรับถอดรหัสข้อมูล (Decrypt) ทั้งหมดกลับคืนมา ซึ่งไม่รับประกันการได้ข้อมูลคืน หรือต้องยอมเสียไฟล์ที่ถูกเข้ารหัสโดยการล้างระบบและข้อมูลในเครื่องคอมพิวเตอร์ (Format) ดังนั้น เพื่อเป็นการป้องกันข้อมูลสำคัญในระบบคอมพิวเตอร์และการแพร่กระจายของมัลแวร์ดังกล่าว ผ่านช่องโหว่หรือจุดอ่อนของระบบปฏิบัติการ Microsoft Windows ซึ่งเครื่องคอมพิวเตอร์ส่วนใหญ่ของหน่วยงานในสังกัดกรมที่ดินใช้ระบบปฏิบัติการดังกล่าว จึงเห็นควรให้เจ้าหน้าที่ของส่วนราชการในสังกัดกรมที่ดินทุกระดับ ดำเนินการตามแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดิน ***(เอกสารหมายเลข ๕)*** อย่างเคร่งครัด และกรณีเฉพาะกิจในการป้องกันและการแก้ไขเมื่อติดมัลแวร์เรียกค่าไถ่ (Ransomware) ชื่อ WannaCry ***(เอกสารหมายเลข ๖)*** ให้ดำเนินการโดยเร่งด่วน ดังนี้

๓.๑ การบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบคอมพิวเตอร์

๓.๑.๑ ให้สำรองข้อมูล (Backup Data) ในเครื่องคอมพิวเตอร์แม่ข่าย (Server) ตามแผนปฏิบัติการอย่างสม่ำเสมอ และตรวจสอบการกู้คืนระบบ (Restore)

๓.๑.๒ ปรับปรุงช่องโหว่หรือจุดอ่อนของระบบปฏิบัติการ Microsoft Windows (Update Patch) และปรับปรุงโปรแกรมพื้นฐานที่ฝังตัวอยู่ในฮาร์ดแวร์ (Firmware) ให้เป็นปัจจุบัน และในกรณีระบบหรือเครื่องคอมพิวเตอร์แม่ข่ายที่มีการจ้างบำรุงรักษา จะต้องมีการตรวจสอบให้บริษัทผู้รับจ้างทำการ Update Patch ระบบปฏิบัติการ และปรับปรุง Firmware ของระบบให้เป็นปัจจุบัน **ทั้งนี้** ให้มีการทดสอบการทำงานของระบบที่เกี่ยวข้องทุกฟังก์ชัน ถึงผลกระทบในการดำเนินงาน

๓.๑.๓ ปิดการ...

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

๓.๒ การบริหารจัดการเครื่องคอมพิวเตอร์ลูกข่าย และระบบคอมพิวเตอร์ของส่วนราชการในสังกัดกรมที่ดิน

๓.๒.๑ แนวทางการป้องกันการติดมัลแวร์เรียกค่าไถ่

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

๒) ปรับปรุงช่องโหว่หรือจุดอ่อนของระบบปฏิบัติการ Microsoft Windows (Update Patch)

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

๓.๒.๒ วิธีการจัดการเมื่อติดมัลแวร์เรียกค่าไถ่

๑) ให้ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อกับระบบเครือข่ายสื่อสารของกรมที่ดินและเครือข่ายอินเทอร์เน็ตในทันที โดยการถอดสาย LAN ออก และปิด Wi-Fi

๒) ทำการ Format เครื่องคอมพิวเตอร์ทุกไดรฟ์ (Drive) เพื่อล้างข้อมูลทั้งหมด และให้ติดตั้งระบบปฏิบัติการใหม่โดยใช้แผ่น CD หรือ DVD เท่านั้น

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบขอได้โปรดลงนามในหนังสือถึงผู้ว่าราชการจังหวัดทุกจังหวัดที่นำเรียนมาพร้อมนี้ และสำนักเทคโนโลยีสารสนเทศจะได้เวียนแจ้งส่วนราชการในสังกัดกรมที่ดินได้รับทราบ และถือปฏิบัติอย่างเคร่งครัดต่อไป

(นายชาลี ชื่นอุไทย)
ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

- เห็นชอบ
- ลงนามแล้ว

(นายประทีป กีรติเรขา)
อธิบดีกรมที่ดิน
๑๘ พ.ค. ๒๕๖๐