แนวทางการป้องกัน และการรับมือมัลแวร์เรียกค่าไถ่ (Ransomware) ในระบบคอมพิวเตอร์

สำหรับผู้ดูแลระบบ (Admin): เพื่อบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย (Server) เครื่องคอมพิวเตอร์ลูกข่ายของหน่วยงาน และระบบคอมพิวเตอร์

๑. ติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-virus) พร้อม Update ให้เป็นปัจจุบัน และหมั่นสแกน (Scan) ไวรัสคอมพิวเตอร์อยู่เสมอ

๒. ให้สำรองข้อมูล (Backup Data) ในเครื่องคอมพิวเตอร์แม่ข่าย (Server) ตามแผนปฏิบัติการอย่างสม่ำเสมอ พร้อมเข้ารหัสไฟล์ Back up และตรวจสอบการกู้คืนระบบ (Restore)

๓. กำหนด และปรับปรุงการตั้งค่า Configuration ในระบบคอมพิวเตอร์เพื่อป้องกันและรับมือโปรแกรมเรียกค่าไถ่ (Ransomware) ดังนี้

๓.๑ Block blacklist IP จากข้อมูล Threat Intelligence เพื่อเป็นการป้องกันเบื้องต้นในการเข้าถึง Server ต่าง ๆ ที่เป็นอันตราย

๓.๒ ตรวจสอบการเข้าถึงของอุปกรณ์ Security โดยเปิดเฉพาะ Port ที่จำเป็นต้องใช้งานเท่านั้น

๓.๓ ตั้งค่า Group Policy เช่น ไม่ให้ใช้งานไฟล์ที่สามารถ Execution ได้ ปิด Auto-play ต่าง ๆ และกำหนดให้ติดตั้งเฉพาะ Software ที่องค์กรให้ใช้งานเท่านั้น

๓.๔ ปิดมาโครของ Microsoft Office (Macro) เนื่องจาก ไฟล์ Microsoft Office มี Script ที่เริ่มงานทำไฟล์โดยที่ไม่ต้องออกคำสั่ง หากไม่มีความจำเป็นต้องใช้งานแนะนำให้ปิดการใช้งาน

๓.๕ เปิดแสดงนามสกุลไฟล์ (File Type) เนื่องจาก มีหลายครั้งที่อาชญากรไซเบอร์ซ้อนนามสกุลไฟล์ เช่น .pdf หรือ .exe เพื่อซ่อนนามสกุลไฟล์จริงเอาไว้ ดังนั้น ควรเปิดการแสดงนามสกุลไฟล์เพื่อให้ผู้ใช้งานสามารถสังเกตเห็นความผิดปกติ

๓.๖ กรองไฟล์แนบในอีเมล (e-mail Attachments) หากองค์กรมีซอฟต์แวร์รักษาความปลอดภัยที่มีฟังก์ชันกรองอีเมลให้กรองไฟล์ที่มีนามสกุล “.exe” เพื่อคัดกรองอีเมลที่มีนามสกุล “.exe” ออกไป

๓.๗ ปิดระบบรีโหมด (Disable RDP) โปรแกรมเรียกค่าไถ่สามารถเข้ามาทางระบบสั่งการระยะไกล หรือ Remote Desktop Protocol (RDP) ที่อนุญาตให้คุณสามารถเข้าถึงคอมพิวเตอร์จากระยะไกล และหากไม่ได้ใช้งานอยู่แล้ว ให้ปิดไว้

๓.๘ ปรับปรุงช่องโหว่หรือจุดอ่อนของระบบปฏิบัติการ Microsoft Windows (Update Patch) และปรับปรุงโปรแกรมพื้นฐานที่ฝังตัวอยู่ในฮาร์ดแวร์ (Firmware) ให้เป็นปัจจุบัน และในกรณีไม่สามารถ Patch ได้ในทันทีควรทำการ Disable: SMBv1 (Server Message Block) หากไม่ได้ใช้งาน

๓.๙ ปิดการใช้งาน SMBv1 (Server Message Block) ของระบบปฏิบัติการ Microsoft Windows เพื่อป้องกันช่องโหว่ของ SMB เวอร์ชั่น ๑ ซึ่งเป็นช่องทางในการแพร่กระจายตัวเองของ Ransomware

๔. อบรมความรู้เกี่ยวกับภัยคุกคามทาง Internet เช่น ภัยที่มาจาก E-mail เป็นต้น

สำหรับผู้ใช้งาน: เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ลูกข่าย และระบบคอมพิวเตอร์ของหน่วยงาน

๑. แนวทางการป้องกันการติดมัลแวร์เรียกค่าไถ่

๑.๑ ติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-virus) พร้อม Update ให้เป็นปัจจุบัน และหมั่นสแกน (Scan) ไวรัสคอมพิวเตอร์อยู่เสมอ

๑.๒ ให้สำรองไฟล์ข้อมูล (Back up) ในเครื่องคอมพิวเตอร์เป็นประจำทุกวันอย่างสม่ำเสมอ โดยควรเก็บข้อมูลที่ทำการสำรองไว้ในอุปกรณ์อื่นใดภายนอกเครื่องคอมพิวเตอร์ หรือจัดเก็บไว้หลายแห่ง

๑.๓ ไม่ควรคลิกลิงก์ หรือเปิดไฟล์ที่แนบมาพร้อมกับอีเมลที่น่าสงสัย หากไม่มั่นใจไฟล์ หรืออีเมลว่ามาจากแหล่งที่น่าเชื่อถือได้ หรือไม่รู้จักผู้ส่งอีเมล ให้ลบทิ้งไป และควรดาวน์โหลดซอฟต์แวร์จากแหล่งที่น่าเชื่อถือได้เท่านั้น

๑.๔ ปรับปรุงช่องโหว่หรือจุดอ่อนของระบบปฏิบัติการ Microsoft Windows (Patch)

๑.๕ 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

๓. สิ่งที่ควรทำทุกเดือน (End user/Admin)

๓.๑ ตรวจสอบทุกเดือน เช่น ช่องโหว่ของ OS และ หมั่น Update Patch สม่ำเสมอ

๓.๒ กำหนดสิทธิการเข้าถึงไฟล์ที่สำคัญให้ได้เพียง Read-only เท่านั้น และหมั่นตรวจสอบการเข้าถึงไฟล์หรือ Folder เมื่อไม่มีการใช้งาน ให้ยกเลิกการแชร์ไฟล์ด้วย

๓.๓ ไฟล์หรือ Folder ที่สำคัญ ให้กำหนดสิทธิการเข้าถึงจากบุคคลภายนอกให้เพียง Read-only เท่านั้น

๓.๔ สำรองไฟล์ข้อมูล (Backup)

เหตุผลที่ผู้เชี่ยวชาญส่วนใหญ่แนะนำไม่ให้จ่ายเงินค่าไถ่

๑. การจ่ายเงินค่าไถ่จะเป็นการสนับสนุนให้อาชญากรทำการฉ้อโกงแบบนี้ต่อไป

๒. ไม่มีการรับประกันว่าเมื่อจ่ายเงินค่าไถ่ไปแล้ว คุณจะได้รับไฟล์ของคุณกลับคืนมา

กรณีติดไวรัสคอมพิวเตอร์ สามารถประสานงานขอคำแนะนำ หรือความช่วยเหลือจาก
สำนักเทคโนโลยีสารสนเทศ ทางโทรศัพท์หมายเลข ๐ - ๒๕๐๓-๒๑๑๐ - ๙ ต่อ ๔๐๕ หรือ ๔๐๗
หรือ ๐ - ๒๕๐๓ - ๓๓๖๙ หรือ ๐ – ๒๙๘๔ - ๐๘๖๐
หรือโทรศัพท์ผ่านระบบอินเทอร์เน็ต (VoIP): ๐๐๐๐๐๑ - ๓ หรือ ๐๐๐๐๑๐ – ๑๑ หรือ ๐๐๐๐๑๓

ที่มา: https://www.catcyfence.com/it-security/article/what-is-ransomware-and-how-to-protect/
และ ESET NOD32 Antivirus