ธนาคารแห่งประเทศไทย

26 กันยายน 2559

เรียน ผู้จัดการ

ธนาคารพาณิชย์ทุกแห่ง
สถาบันการเงินเฉพาะกิจทุกแห่ง

ที่ ธปท.ฝตส.(03) ว. 1180 /2559 เรื่อง แนวปฏิบัติในการป้องกันความเสี่ยงของระบบ ATM จากโปรแกรม Malware

ระบบ ATM เป็นช่องทางการทำธุรกรรมการเงินทางอิเล็กทรอนิกส์หลักที่ประชาชนมีการใช้บริการในวงกว้าง การพัฒนาระบบการรักษาความปลอดภัยให้รองรับภัยคุกคามใหม่ ๆ จะช่วยให้การบริการแก่ลูกค้าประชาชนเป็นไปอย่างต่อเนื่อง มีความปลอดภัยและเกิดความเชื่อมั่นในการใช้บริการ ปัจจุบันภัยคุกคามระบบ ATM จากโปรแกรม Malware มีแนวโน้มเพิ่มมากขึ้น สถาบันการเงิน (สง.) จำเป็นต้องยกระดับการป้องกันความเสี่ยงเพื่อให้สามารถรับมือกับภัยคุกคามดังกล่าวได้อย่างทันการณ์ ธปท. จึงได้กำหนดแนวปฏิบัติในการป้องกันความเสี่ยงของระบบ ATM จากโปรแกรม Malware ให้ สง. ถือปฏิบัติประกอบด้วย มาตรการระยะสั้นและระยะยาว มีสาระสำคัญดังนี้

1. **มาตรการระยะสั้น** ครอบคลุมการตรวจสอบสภาพความเรียบร้อยของตู้ ATM อุปกรณ์เครือข่ายสื่อสาร กล้องวงจรปิด และบริเวณโดยรอบอย่างเคร่งครัด ควบคุมการจัดเก็บและเบิกใช้กุญแจตู้ ATM การปรับแต่งค่าความปลอดภัยของระบบที่ตู้ ATM และอุปกรณ์เครือข่ายสื่อสาร รวมทั้งปรับปรุงการควบคุมการเติมเงิน และการกระทบยอดเงินที่ตู้ ATM ให้รัดกุมยิ่งขึ้น โดยตามมาตรการระยะสั้น สง. ควรดำเนินการให้แล้วเสร็จภายใน 6 เดือน

2. **มาตรการระยะยาว** ครอบคลุมการปรับปรุงตู้ ATM และระบบที่เกี่ยวข้องกับการให้บริการ ATM เพื่อเพิ่มขีดความสามารถในการป้องกันและติดตามภัยคุกคาม รวมทั้งการปรับปรุงการควบคุมการปฏิบัติงานที่ตู้ ATM ให้เคร่งครัดรัดกุมยิ่งขึ้น เช่น ในด้านการติดตั้งโปรแกรมที่ตู้ ATM ตลอดจนมีระบบที่คอยตรวจจับสิ่งผิดปกติ เช่น ตู้ ATM ถูกเปิดหรือถูกงัดแงะ การรีบู๊ตในลักษณะที่ไม่ได้วางแผนไว้ล่วงหน้า (Unplanned Reboot) เป็นต้น โดยมาตรการระยะยาว สง. ควรดำเนินการให้แล้วเสร็จภายใน 2 ปี

ทั้งนี้ ขอให้หน่วยงานด้านการกำกับการปฏิบัติงานและหน่วยงานตรวจสอบภายในของ สง. มีส่วนร่วมในการกำกับดูแลและประเมินการปฏิบัติตามแนวปฏิบัติดังกล่าว และขอให้ สง. ส่งผลการประเมินพร้อมทั้งแผนการพัฒนาและปรับปรุงตามแนวปฏิบัติฉบับนี้ มายังฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ สายกำกับสถาบันการเงิน ธนาคารแห่งประเทศไทย (Email: IToffsiteSupervision-RID@bot.or.th) ภายใน 60 วัน นับจากวันที่หนังสือฉบับนี้ลงนาม

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นายรณดล นุ่มนนท์)
ผู้ช่วยผู้ว่าการ สายกำกับสถาบันการเงิน
ผู้ว่าการแทน

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ
สายกำกับสถาบันการเงิน
โทรศัพท์ 0 2283 6448
โทรสาร 0 2356 7450

แนวปฏิบัติการป้องกันความเสี่ยงของระบบการให้บริการ ATM จากโปรแกรม Malware

ธนาคารแห่งประเทศไทย (ธปท.) ตระหนักถึงความสำคัญในการยกระดับการรักษาความปลอดภัยระบบ ATM เพื่อให้มีความปลอดภัยและพร้อมรับมือกับภัยคุกคามที่เกิดขึ้นอย่างต่อเนื่อง โดยเฉพาะที่พบมากที่สุด คือภัยคุกคามจาก Malware ธปท. จึงได้กำหนดแนวปฏิบัติในการป้องกันความเสี่ยงของระบบ ATM จากโปรแกรม Malware ซึ่งประกอบด้วยมาตรการระยะสั้นและระยะยาว ดังนี้

1. มาตรการระยะสั้น

(1) ตรวจสอบสภาพความเรียบร้อยของตู้ ATM และบริเวณโดยรอบอย่างเคร่งครัด เพื่อให้มั่นใจว่าตู้ ATM และอุปกรณ์เครือข่ายสื่อสารของตู้มีการควบคุมและรักษาความปลอดภัยทางกายภาพอย่างเพียงพอ เช่น การปิดล็อคตู้ ATM และอุปกรณ์เครือข่ายสื่อสารอย่างปลอดภัย เพื่อป้องกันการติดตั้งอุปกรณ์แปลกปลอมที่ตู้หรือการถูกงัดแงะตู้ ATM แสงไฟและความสว่างของบริเวณโดยรอบเพียงพอ โดยสถาบันการเงินควรจัดให้มี Checklist เพื่อให้เจ้าหน้าที่ใช้เป็นมาตรฐานในการตรวจสอบ

(2) ตรวจสอบความเพียงพอและคุณภาพของกล้องวงจรปิดที่ตู้ ATM (เช่น จำนวนกล้อง มุมกล้อง และความชัดเจน) เพื่อให้มั่นใจว่าสามารถบันทึกเหตุการณ์ที่จะใช้เป็นหลักฐานในการดำเนินคดีอย่างเพียงพอ

(3) ปรับปรุงการควบคุมกระบวนการจัดเก็บและเบิกใช้กุญแจตู้ ATM และอุปกรณ์เครือข่ายสื่อสาร เพื่อป้องกันการนำกุญแจไปใช้โดยไม่ได้รับอนุญาต

(4) ควบคุมการเข้าถึงและการรักษาความปลอดภัยโปรแกรม BIOS ของตู้ ATM ดังนี้

(4.1) เปลี่ยน Default BIOS Password ที่มากับตู้ ATM โดยสถาบันการเงินควรกำหนดรหัสผ่านแต่ละตู้ให้แตกต่างกัน (Unique) หากสามารถดำเนินการได้ เพื่อให้มีความปลอดภัยมากยิ่งขึ้น

(4.2) ควบคุมดูแลการจัดเก็บและการเบิกใช้ BIOS Password อย่างรัดกุมปลอดภัย โดยสถาบันการเงินเป็นผู้ควบคุมดูแลเอง รวมถึงมีหลักฐานสามารถตรวจสอบได้ในภายหลัง

(4.3) ตั้งค่าระบบ BIOS ไม่ให้มีการอัพเดทแบบอัตโนมัติ (Automatic BIOS Update) รวมถึงให้ปิดทุกช่องทางที่สามารถเชื่อมต่อกับอุปกรณ์ภายนอก เช่น CD-ROM, Floppy Disk, USB เป็นต้น และกำหนดให้บู๊ตระบบปฏิบัติการผ่านทาง Primary Harddisk เท่านั้น

(5) ควบคุมการเข้าถึงและการรักษาความปลอดภัยระบบปฏิบัติการ (Operating System) ของตู้ ATM ดังนี้

(5.1) ติดตั้งระบบควบคุมเพื่อให้โปรแกรมที่ได้รับอนุญาตเท่านั้นสามารถทำงานบนตู้ ATM ได้ เช่น การควบคุมโดยใช้โปรแกรม Whitelisting เป็นต้น

(5.2) เปลี่ยน Default Password ที่มากับ Core PC ของตู้ ATM โดยสถาบันการเงินควรกำหนดรหัสผ่านแต่ละตู้ให้มีความแตกต่างกัน (Unique) หากสามารถดำเนินการได้ เพื่อให้มีความปลอดภัยมากยิ่งขึ้น

(5.3) ทบทวนและควบคุมดูแลสิทธิ์ผู้ใช้งานให้เหมาะสมตามความจำเป็นของการใช้งานบน Core PC ของตู้ ATM โดยมีกระบวนการควบคุมการเบิกใช้งานสิทธิ์ที่รัดกุมและสามารถตรวจสอบได้ในภายหลัง

(5.4) สอบทานและปรับแต่งค่าความปลอดภัยของ Core PC ให้มีความรัดกุมปลอดภัย (Hardening) โดยควรครอบคลุมการปฏิบัติอย่างน้อยดังต่อไปนี้

- ปิดหรือลบโปรแกรมและ Services ที่ไม่ได้ใช้งานและมีความเสี่ยงต่อการเข้าถึงระบบ เช่น Web Browser, Download Program, Command Prompt, Notepad, File Sharing, Shortcut, Hotkey, Auto-Play, Dumb-File Creation, Start Bar/Tray Menu, Key Combinations, การเชื่อมต่อกับ Wi-Fi และ Bluetooth เป็นต้น
- เปิด Firewall Services บน Core PC เพื่อคัดกรองการติดต่อสื่อสาร
- ตั้งค่าให้มีการลบแคชโดยอัตโนมัติ (Cache Auto-deletion) เพื่อไม่ให้มีการจดจำข้อมูลที่สำคัญ
- จัดเก็บ Security Log และ Event Log ของ Core PC ตู้ ATM

(6) ควบคุมการเข้าถึงและการรักษาความปลอดภัยอุปกรณ์เครือข่ายสื่อสาร (Router) ที่ตู้ ATM ดังนี้

(6.1) เปลี่ยน Default Password ของอุปกรณ์เครือข่ายสื่อสาร โดยควรกำหนดรหัสผ่านของอุปกรณ์เครือข่ายสื่อสารให้แตกต่างกัน (Unique) เพื่อให้ปลอดภัยมากยิ่งขึ้น

(6.2) ทบทวนและควบคุมดูแลสิทธิ์ผู้ใช้งานให้เหมาะสมตามความจำเป็นของการใช้งานบนอุปกรณ์เครือข่ายสื่อสาร โดยมีกระบวนการควบคุมการเบิกใช้งานสิทธิ์ที่รัดกุมและสามารถตรวจสอบได้ในภายหลัง รวมทั้งควรเปลี่ยนรหัสตามรอบระยะเวลาที่เหมาะสม

(6.3) สอบทานและปรับแต่งค่าความปลอดภัยของอุปกรณ์เครือข่ายสื่อสาร (Router) ที่ตู้ ATM เชื่อมต่อมายังระบบส่วนกลางให้รัดกุมปลอดภัย (Hardening) โดยควรครอบคลุมการปฏิบัติอย่างน้อยดังต่อไปนี้

- ปิดพอร์ตการเชื่อมต่อและ Service ที่ไม่ได้ใช้งาน
- อนุญาตให้เครื่องที่ได้รับอนุญาตเท่านั้น ที่สามารถเชื่อมต่อเข้ามายังเครือข่าย
- จัดเก็บ Security Log และ Event Log ของอุปกรณ์เครือข่ายสื่อสาร

(7) ทบทวนและปรับปรุงกระบวนการเติมเงินที่ตู้ ATM โดยต้องมีการควบคุมการปฏิบัติงานของเจ้าหน้าที่ ซึ่งรวมถึงการใช้บริการจากผู้ให้บริการภายนอกให้เป็นไปตามหลักการควบคุมภายในที่ดี ได้แก่ การแบ่งแยกหน้าที่ (Segregation of duties) การควบคุมแบบ Dual control และการสอบทานการปฏิบัติงานโดยเจ้าหน้าที่สถาบันการเงินที่มีความเป็นอิสระอย่างสม่ำเสมอ

(8) ทบทวนและปรับปรุงกระบวนการกระทบยอดเงินที่ตู้ ATM เพื่อให้สามารถตรวจพบความผิดปกติของปริมาณเงินสดในตู้ ATM ได้อย่างทันการณ์

2. มาตรการระยะยาว

(1) ควรดำเนินการปรับปรุงการควบคุมและรักษาความปลอดภัยตู้ ATM ดังต่อไปนี้

(1.1) จัดให้มีกระบวนการจัดการกุญแจตู้ ATM ที่มีความรัดกุมปลอดภัยสอดคล้องตามหลักการแบ่งแยกหน้าที่ และสามารถตรวจสอบได้ในภายหลัง รวมทั้ง ควรจัดให้มีมาตรฐานและกระบวนการสอบทานการปฏิบัติงานที่ตู้ ATM ของเจ้าหน้าที่อย่างสม่ำเสมอและเพียงพอ

(1.2) จัดให้มีการ Pairing Authentication ระหว่างเครื่องจ่ายเงินและ Core PC ของตู้ ATM เพื่อป้องกันการสั่งจ่ายเงินจากอุปกรณ์คอมพิวเตอร์อื่น นอกจากนี้ให้เลือกใช้ตู้ ATM ที่มีระบบควบคุม Core PC แยกออกจากเครื่องจ่ายเงิน หากสามารถดำเนินการได้ เพื่อเพิ่มระดับการควบคุมการเข้าถึงให้ปลอดภัยมากยิ่งขึ้น

(1.3) เข้ารหัสข้อมูลในฮาร์ดดิสก์ (Harddisk) ของตู้ ATM ด้วยวิธีการเข้ารหัสที่ปลอดภัยและทันสมัย (Full Harddisk Encryption)

(1.4) ปรับปรุง (Update/Patch) ระบบปฏิบัติการของ Core PC และอุปกรณ์เครือข่ายสื่อสารให้ทันสมัยและเป็นไปตามคำแนะนำของผู้ผลิต

(2) แบ่งแยกเครือข่ายระบบ ATM ออกจากระบบเครือข่ายภายในอื่น ๆ ของสถาบันการเงิน และควบคุมการเชื่อมต่อระหว่างตู้ ATM ระบบ Software Distribution Management System (ระบบ SDMS) และระบบ ATM Host พร้อมทั้งกำหนด Access Control List เพื่อป้องกันความเสี่ยงของภัยคุกคามทางระบบเครือข่าย เช่น IP Spoofing เป็นต้น

(3) จัดให้มีระบบการพิสูจน์ตัวตนของการติดต่อสื่อสารระหว่างระบบ SDMS และตู้ ATM ด้วยวิธีการที่ปลอดภัยและสามารถป้องกันภัยคุกคาม เช่น IP Spoofing, Man in the middle attack เป็นต้น

(4) จัดให้มีการเข้ารหัสช่องทางการติดต่อสื่อสารจากตู้ ATM มายังระบบส่วนกลางด้วยมาตรฐานโปรโตคอลที่ปลอดภัย โดยสถาบันการเงินจัดให้มีมาตรฐานและกระบวนการบริหารจัดการ Key ที่ใช้ในการเข้ารหัสอย่างรัดกุมปลอดภัย

(5) ควบคุมดูแลความปลอดภัยของระบบ SDMS โดยควรครอบคลุมการปฏิบัติอย่างน้อยดังต่อไปนี้

(5.1) ตรวจหา (Scan) และกำจัด Virus/ Malware ที่พบ พร้อมทั้งดำเนินการติดตั้งและปรับปรุง Anti-Virus/Anti-Malware บน Server อย่างสม่ำเสมอ

(5.2) เปลี่ยน Default Password ของระบบ SDMS เพื่อให้ปลอดภัยมากยิ่งขึ้น

(5.3) ทบทวนและควบคุมดูแลสิทธิ์ผู้ใช้งานบนระบบ SDMS ให้เหมาะสมตามความจำเป็นของการใช้งาน โดยมีกระบวนการควบคุมการเบิกใช้สิทธิ์ที่รัดกุมและสามารถตรวจสอบได้ภายหลัง รวมทั้งควรเปลี่ยนรหัสตามรอบระยะเวลาที่เหมาะสม

(5.4) ปรับแต่งค่าความปลอดภัยของระบบให้รัดกุมปลอดภัย (Hardening) อย่างสม่ำเสมอ เพื่อไม่ให้มีช่องโหว่จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต พร้อมทั้งตรวจสอบให้มั่นใจว่าระบบมีการจัดเก็บ Security Log และ Event Log อย่างเพียงพอ

(6) จัดให้มีระบบในการแจ้งเตือนความผิดปกติของตู้ ATM ทั้งในลักษณะ Physical, Logical และ Network attacks เช่น ตู้ ATM ถูกเปิดหรือถูกงัดแงะ ถูกติดตั้งอุปกรณ์หรือโปรแกรมแปลกปลอมที่ตู้ การรีบู๊ตในลักษณะที่ไม่ได้วางแผนไว้ล่วงหน้า (Unplanned Reboot) เป็นต้น โดยระบบควรแจ้งเตือนไปยังเจ้าหน้าที่เพื่อให้สามารถดำเนินการติดตามตรวจสอบได้อย่างทันท่วงที

(7) ทบทวนและปรับปรุงกระบวนการติดตั้งระบบที่ตู้ ATM โดยควรครอบคลุมการปฏิบัติอย่างน้อยดังต่อไปนี้

(7.1) มีการควบคุมให้ผู้ที่ได้รับอนุญาตเท่านั้นมีสิทธิ์ในการเข้าถึงชุดโปรแกรม Master ที่จะนำไปใช้ในการติดตั้งที่ตู้ ATM

(7.2) มีกระบวนการในการตรวจสอบโปรแกรม Virus/Malware ที่ชุดโปรแกรม Master ก่อนนำไปติดตั้ง

(7.3) มีการควบคุมและสอบทานการปฏิบัติงานของเจ้าหน้าที่ที่ไปปฏิบัติงานที่ตู้ ATM เป็นประจำ