金融機構提供自動櫃員機系統安全作業規範

本會 105 年 12 月 22 日第 12 屆第 2 次理監事聯席會議通過
金管會 106 年 2 月 13 日金管銀國字第 10600014760 號函洽悉
本會 107 年 1 月 25 日第 12 屆第 14 次理監事聯席會議通過
金管會 107 年 5 月 15 日金管銀國字第 10702042100 號函洽悉
本會 114 年 5 月 29 日第 14 屆第 25 次理監事聯席會議通過
金管會 114 年 7 月 9 日金管銀國字第 1140219887 號函修正後洽悉

第一條 目的

金融機構提供自動櫃員機(以下簡稱 ATM)服務，除符合「金融機構辦理電子銀行業務安全控管作業基準」外，為確保金融機構 ATM 系統安全，特定本作業規範。

第二條 用詞定義如下：

一、 兩項以上技術：係指「金融機構辦理電子銀行業務安全控管作業基準」之兩項以上技術相關規定。

二、 ATM 之相關伺服器：係指與 ATM 網路連接並提供服務，如派版伺服器負責安裝或更新 ATM 內檔案或修改 ATM 環境設定、監控伺服器負責監控 ATM 實體或系統執行狀態、安全更新伺服器負責更新 ATM 作業系統或應用程式、防毒伺服器負責更新防毒軟體或病毒碼、網域控制伺服器負責管理網域存取權限、白名單伺服器負責管理 ATM 檔案存取權限等。

第三條 開發測試

一、 開發單位應以 ATM 應用程式進行原始碼掃描並提供掃描報告。

二、 開發單位應以兩人以上授權或採用兩項以上技術進行版本控管，並交付派版程式清單、程式異動前後差異比對表、程式變更內容及原始碼掃描報告。

三、 金融機構應檢視、測試及風險評估後，依據原始碼掃描報告，判定是否進行派版。

第四條 交付派版

一、 派版單位應驗證開發單位交付檔案之完整性(如 MD5)及來源辨識性(如 ZIP 加密)。

二、 派版單位應掃描開發單位交付檔案有無惡意程式(如病毒、插件、後門等)。

三、 派版單位應於派版後進行覆核作業，確保無不當派版情形。

第五條 存取限制

一、 應刪除 ATM 不必要之作業系統服務及應用程式(如附件)。

二、 應禁止 ATM 之作業系統啟用 AutoPlay 功能。

三、 採用 IP 連線之 ATM 其可執行程式應建立白名單管控，白名單異動作業應經兩人以上授權或採用兩項以上技術進行管控；異動 ATM 可執行程式前，ATM 應驗證異動作業來源正確性。

四、 以具異動權限之帳號登入派版伺服器、監控伺服器及安全更新伺服器之作業系統或應用程式者應採用兩人以上授權或採用兩項以上技術進行管控。

五、 ATM BIOS 應指定可開機之儲存媒體並移除不必要之設備（如 CD-ROM 或外接式儲存媒體)。

六、 本款規定公布後新採購之 ATM，其吐鈔模組與 ATM 控制主機間之通訊指令應受保護並具有授權機制，以防止植入未經授權程式、竄改指令或竄改韌體。

第六條 架構區隔

一、 應透過設備隔離機制(如防火牆、虛擬私有網路（Virtual Private Network，VPN)、網閘等)管制 ATM、ATM 之相關伺服器，其中針對 ATM 及 ATM 之相關伺服器應限制不得連接網際網路、開發測試網段及內部辦公區網段，惟防毒伺服器及網域控制伺服器因提供服務之目的(如更新病毒碼、時間校時、DNS 查詢、身分確認等)除外。

二、 執行派版作業之工作站應設置於經管制之作業室，且不得連接網際網路。

三、 ATM 之派版伺服器僅能於執行作業(如 ATM 派版、資安作業、系統更新)時開機或連線，並於作業完畢後立即關機、離線或停用連線埠，惟增加下列安全防護機制者除外。

（一）僅能透過本機或執行派版作業之工作站登入。

（二）依最小授權原則進行派版伺服器各項安全控管設定(如派版功能僅限授權派版專用帳號)。

（三）採用兩項以上技術進行身分確認，並使用硬體設備保護敏感

資料；該硬體設備應具有資料輸出管控機制、遮蔽作用之塗層保護機制、破壞偵測與歸零清除保護機制、開機自我測試機制、防止電磁干擾保護機制或其他足以保護設備內敏感資料之安全設計(如動態密碼產生器)。

第七條 監控警示

一、 應監控 ATM、ATM 之相關伺服器及網路設備之系統事件及連線紀錄，如有異常應及時處理。

二、 連線至 ATM 派版伺服器之工作站與其他網段之資料傳遞，應留存連線紀錄以利追蹤異常存取。

第八條 汰換計畫

採用 IP 連線之 ATM，若該設備之作業系統原廠已不再提供安全更新者，金融機構應提出汰換計畫，並提報董(理)事會或經其授權之經理部門核定，未汰換期間應有補強措施(如採用具 Virtual Patching 功能之 WAF 或 IPS、或採網段隔離機制並限制同網段主機間連線及資源存取)，且應儘速完成補強措施或汰換，以防範已知資安漏洞。

第九條 人工派版

一、 採用 USB、CD-ROM 人工派版者，須由指定人員使用經銀行確認之 ATM 應用程式進行換版。

二、 應定期對指定人員(如保全)進行查核。

第十條 資安防護與演練

一、 ATM 之相關伺服器、伺服器之工作站應安裝防毒軟體，並確認正確來源之病毒碼後即時更新；派版伺服器應先更新病毒碼後再進行作業。

二、 應每半年針對 ATM 相關之伺服器進行弱點掃描。

三、 應建立監控與事故應變機制並每年進行程序演練。

附件：不必要之作業系統服務及應用程式

下表僅提供參考，如有必要使用應導入必要管控機制。

Application	Filename	Description/Purpose
Address Resolution Protocol	arp.exe	Display/edit network address
File Transfer Protocol	ftp.exe	Transfer files between two hosts
NetBios over TCP/IP	nbtstat.exe	Display network information
Name Server Lookup	nslookup.exe	Display network information
Remote Copy Program	rcp.exe	Copy files
TCP/IP Route Command Application	route.exe	Display/edit network settings
Remote Shell Application	rsh.exe	Execute command on remote computer
Terminal Emulation Protocol	telnet.exe	Connect to a remote computer