數位發展部資通安全署
Administration for Cyber Security, moda

中小企業基本資安防護指引

115 年 3 月

目錄

中小企業基本防護指引

基本資安防護指引 × 自評檢核

中小企業常存有「公司規模小，不是駭客目標」的迷思，然而，這已成為企業最致命的資安盲點。事實上，由於中小企業常被認為資源有限、安全實作相對不足，反而容易成為駭客的主要目標，常見攻擊型態包括釣魚郵件、詐騙訊息、勒索軟體等，因此，建議中小企業優先以三個面向著手投入資安防護：

01 帳號管理

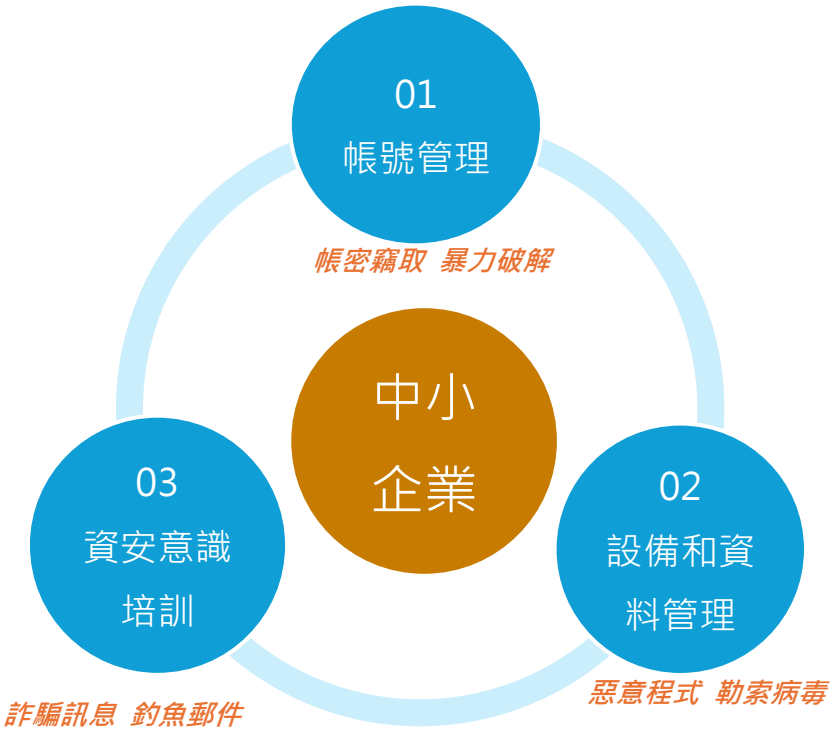
為重要系統帳號啟用二階段驗證(2FA)、建立帳號與權限管理機制、定期檢視及移除不必要帳號

02 設備和資料管理

定期更新作業系統與應用程式、安裝並啟用防毒或管控外接裝置 (如 USB)

03 資安意識培育

定期進行資安宣導、提醒釣魚郵件辨識、建立基本通報觀念



01 帳號管理

防護措施指引

(一) 使用強密碼或密碼短語｜使用「長」、「複雜」、「不重複使用」的密碼，建議至少 15 碼，並可利用密碼短語，或由多個單子組成，以便使用者易於記憶且符合強度建議，另外，亦可使用密碼管理工具生成及管理密碼。

(二) 啟用二階段驗證｜2FA 是在使用者登入時要求額外的一種或多種身分鑑別方式，例如生物辨識、使用手機 App 取得代碼、簡訊（SMS）驗證碼等，即使密碼被竊取時，駭客也無法輕易登入。

(三) 實施存取控制｜僅授予員工「完成其工作所需的最低權限」，關閉不必要的功能，以符合「最小權限原則」（Principle of Least Privilege）。

(四) 帳號獨立與權限管理｜每位員工配發獨立帳號禁止多人共用，員工離職當天即註銷所有系統帳號與權限，定期檢視並清除閒置帳號。

為什麼需要防護？

- 駭客使用自動化工具，針對常見字串(如123456、統編、電話)進行每秒數萬次掃描猜測 ➔**若密碼低於 15 碼且缺乏複雜度，帳號很容易被破解**
- 即便密碼外洩，若缺乏第二道身分驗證，駭客即可長驅直入公司內部系統，甚至竄改密碼讓你無法登入 ➔**未啟用二階段驗證(2FA)，就像是有鎖門卻沒鎖保險箱**
- 多名員工共用帳號，一旦遭竊或發生資安事故，變成無法追蹤及無法找出真正的入侵者 ➔**共用帳號像全公司共用一把鑰匙，只要鑰匙掉了，不知是誰弄丟、無法追蹤**

如何應用

- ✓ **雲端辦公室：在 Google、Microsoft 365 等常用辦公軟體，強制啟用二階段驗證(2FA)**
- ✓ **遠端存取：從外部連回公司 VPN，必須通過多重驗證，防止密碼遭竊導致內網門戶大開**
- ✓ **關鍵系統：在財務系統、ERP、人資系統等高機密平台，設定至少 15 碼的高複雜度密碼**
- ✓ **內部主機管理：嚴禁人員共用 admin、root 帳號，要求管理員使用獨立帳號以便紀錄軌跡**
- ✓ **資料夾存取控管：依照職務設置權限，非該部門人員禁止存取，實現最小權限配置**
- ✓ **入職/離職流程： 建立「人事異動資安核對表」；離職當天，HR 應同步通知 IT 立即停用/刪除 AD 帳號、信箱及雲端空間權限**
- ✓ **合作對象管理： 針對外部協力廠商提供的「臨時帳號」，應設定過期自動關閉機制**
- ✓ **登入紀錄稽核： 定期查看系統是否有「半夜登入」或「異常地點登入」的失敗紀錄**

威脅案例分析 >_ 帳密竊取

◆ 如何因一個「萬用密碼」賠掉，公司一整年的利潤 (> 專業服務業)

某企業為了方便，將公司的印表機與網路主機，服務帳號都設「公司統編」為密碼。駭客 1 分鐘內就破解密碼，成功潛入公司內部網路。駭客進入公司內網後，發現所有系統權限都一樣，就拿著「萬用鑰匙」在公司的帳號管理系統中四處橫行，把自己變成「隱形管理員」。隱匿多時，已掌握公司運作狀況，在某天大半夜對全公司電腦進行「暴力破解」，導致 AD 系統因負載過重與大量登入失敗而不斷當機，隔天上班時，全公司發現每個人無法登入系統、生產線停擺 8 小時。**最終，該公司不僅支付了昂貴的系統重構費用，還因客戶資料外洩，面臨法律訴訟與合約賠償。**

> 營運中斷損失 | 停工 3 天，約損失 NT$ 900 萬

> 數位鑑識與緊急復原費 | 資安公司進場清查，約損失 NT$ 100~300 萬

> 行政罰鍰 | 未盡安全維護義務的企業，罰鍰 NT$2~200 萬元(視情節輕重)

防護案例分析>_ 側錄破解

◆ 一場原本會發生的百萬災難，如何被 3 秒鐘的動作化解(> 專業服務業)

某企業的業務經理參與外部研討會，在休息期間收發 Email，誤連與咖啡店名稱相似的「惡意 Wi-Fi」。駭客透過側錄技術，在 5 分鐘內攔截了經理的辦公室帳號與密碼。當天晚上，駭客嘗試從異地登入經理的雲端硬碟，目標是硬碟內存放的「下年度核心客戶專案清單」與「數筆客戶合約資料」。雖然駭客手握正確密碼，但系統偵測到「異常地點登入」，隨即觸發二階段驗證 ，經理手機彈出通知：「有人嘗試在 [異地]登入您的帳號，是否允許？」，**他意識到自己並未操作，果斷按下「拒絕」，因這一個「拒絕」動作，成功把駭客擋在門外，隨後通知公司 IT 人員重設密碼並清查紀錄，確認資料完全無外洩。**

> 預防成本：開啟 2FA 功能 (多數雲端服務為免費或內含) | 無資料外洩

> 守護價值：僅需重設密碼與進行設備掃描 | 成功賠償歸零，避免可能被詐騙、勒索及導致失去客戶信任受損

中小企業網路大學校「資安刊物」參考 https://www.smelearning.org.tw/publication.php

02 設備和資料管理

防護措施指引

(一) 定期更新軟體｜開啟作業系統及應用程式等軟體自動更新設定，修復安全性漏洞，並定期檢視版本資訊，如已無法更新應考慮替換原有產品。

(二) 導入防毒軟體｜使用防毒軟體檢測設備中的惡意軟體，並定期更新病毒碼及掃描系統。

(三) 定期備份資料｜將重要的資料備份，並定期執行備份演練（測試和恢復）計畫，掌握「3-2-1 備份原則」：3 份備份資料、2 種不同儲存媒體、1 份異地存放，且至少 1 份需為離線存放（Air-gapped）。

(四) 檢查物聯網設備安全設定｜物聯網（Internet of Things，IoT）設備（如網路攝影機、印表機、路由器等）應於安裝時立即修改預設密碼，並確認設備連線必要性。

(五) 設備重置後再出售或丟棄｜設備如需出售或丟棄，應利用專業軟體進行系統重置或格式化，若仍有疑慮建議可進行物理性銷毀，避免有心人士盜取資料。

(六) 資訊資產盤點｜資產盤點是所有防護措施的基礎前提，其盤點範圍包含硬體、軟體、服務、系統、資料及人員等，並逐項做好防護措施。

為什麼需要防護？

- 駭客持續掃描網路，找出未更新軟體的漏洞趁機入侵，並嘗試關閉現有防護程式。駭客亦大量掃描仍使用預設帳密的 IoT 設備，輕易取得控制權。
- 員工誤開偽冒客戶信件的附件，惡意程式即植入電腦，無防毒軟體便無法偵測攔截。勒索軟體入侵後加密所有檔案，無離線備份則無法復原。
- 公司不知道內部還有一台老舊的 Windows 7 測試主機連在網路上，駭客從這台無人管理的設備入侵。

➔導致勒索軟體大規模擴散，使全公司電腦陷入癱瘓，或設備淪為跳板，藉此滲透進入公司內部網路

➔機密客戶資料與報價單遭竊取外洩，公司面臨客戶求償與商譽損失

➔該主機成為跳板滲透至核心系統，公司事後才發現這台「被遺忘的電腦」從未更新、從未備份

如何應用

- ✓ **Windows 電腦開啟「自動更新」功能，確保作業系統與安全性修補程式自動安裝，且已停止支援的系統（如 Windows 7、XP）應儘速汰換**
- ✓ **將常用軟體如 Chrome、Adobe Reader、LINE 等設為自動更新，避免員工使用舊版**
- ✓ **全公司電腦統一安裝防毒軟體，並確認病毒碼每日自動更新**
- ✓ **落實 3-2-1 原則：系統資料至少保留 3 份備份、存放在 2 種不同媒體、其中 1 份離線（如外接硬碟拔除存放）**
- ✓ **公司 Wi-Fi 路由器、網路攝影機、網路印表機等設備，安裝後第一步即修改預設帳號密碼**

✓ **建立一份簡易資產清冊（Excel 即可），記錄所有公司的電腦、伺服器、NAS、路由器、IoT 設備的型號、作業系統版本與負責人**

威脅案例分析 >_ 勒索軟體

◆ 一封郵件癱瘓整間工廠，數百 GB 資料一夕蒸發 (> 傳統製造業 / 加工廠)

某中小型加工廠員工收到一封偽裝成客戶詢價單的電子郵件，點開附件後惡意程式悄悄植入電腦。由於該電腦長期未更新作業系統，駭客輕易利用已知漏洞取得控制權，並在內網潛伏數週，逐步摸清公司網路架構與檔案存放位置。某日凌晨，駭客一次性對全公司電腦發動勒索攻擊，將包含財務報表、員工個資、生產製程圖紙與客戶合約等核心資料全數加密。隔天上班時，**所有電腦螢幕顯示勒索訊息，要求支付比特幣贖金，整條生產線被迫全面停擺**。最終，**該工廠因無離線備份，不僅支付了高額贖金仍未能完整復原資料，更面臨客戶轉單與違約求償的連鎖效應**。

> 營運中斷損失 | 停工 5 天，約損失 NT$ 1,500 萬（含趕工與違約罰款）
> 數位鑑識與緊急復原費 | 資安公司進場清查，約損失 NT$ 100~300 萬
> 勒索贖金 | 駭客要求 NT$ 200~500 萬不等，支付後仍無法保證完整解密
> 近年 | 針對製造業的勒索攻擊正以每年超過 60% 的速度激增

勒索軟體防護指南 TWCERT/CC https://www.twcert.org.tw/tw/cp-14-4843-7060c-1.html

防護案例分析>_ 漏洞攻擊

◆ 全公司啟用自動更新後，同一波零日攻擊中成為唯一倖免的供應商(> 傳統製造業)

某中小型精密零件加工廠半年前在 IT 人員建議下，將全公司 Windows 電腦統一開啟自動更新，並將已停止支援的 Windows 7 設備全數汰換為 Windows 11。某月，一波針對製造業的勒索攻擊大規模爆發，駭客利用的正是一個兩週前才被微軟修補的系統漏洞。**由於該工廠所有設備早已自動安裝修補程式，攻擊封包抵達後全數被系統阻擋，生產線毫無影響**。同一供應鏈中三家仍使用舊版系統的協力廠商卻接連中招停工，該工廠反而因產線穩定而承接了轉單訂單。

> 預防成本：開啟自動更新為免費設定+汰換 舊電腦 | 零入侵、零停工
> 守護價值：供應鏈危機中維持正常出貨，獲得品牌客戶信任加分，額外承接轉單

國家資通安全研究院推廣資源 https://s.moda.gov.tw/8WPGTuqkjD6m

03 資安意識培訓面向

防護措施有哪些？

(一) 員工意識提升｜企業員工具備良好的網路安全習慣，是公司抵禦資安威脅的第一道防線，因此員工應盡量具備相關的資安意識，包括：

✓常見的網路安全威脅，如商業電子郵件詐騙和勒索軟體。

✓識別詐騙和網路釣魚攻擊，包含防範 AI 變造影像與聲音之深偽（Deepfake）詐騙。

✓業務特定流程（例如報告可疑電子郵件）。

✓緊急情況下應採取的措施。

✓公務與私人郵件、通訊軟體分開使用。

✓不要用公司 Email 註冊外部服務。

(二) 制定資安事件應變計畫｜為避免資安事件發生時，相關人員因不知所措而錯過黃金處理時間，因此，制定資安事件應變計畫，員工即可花更少時間思考、並爭取更多的時間採取行動，制定計畫應考慮以下議題：

✓資安事件通報流程。

✓個資外洩通報時限規定。

✓應聯繫甚麼單位/人員尋求協助。

✓如何將事件傳達給其他員工、利害關係人或客戶。

✓重要系統中斷服務時應如何恢復並同時確保業務持續運作。

(三)掌握威脅情資｜註冊我國「台灣電腦網路危機處理暨協調中心 TWCERT/CC」會員，妥善利用其免費服務：

✓接收最新威脅警報：訂閱電子報，獲取即時情資。

✓使用惡意檔案檢測：上傳可疑檔案，協助識別其安全性。

✓通報資安事件：在發生事件時，可尋求 TWCERT/CC 的協調與協助。

為什麼需要防護？

- 駭客針對企業員工發送仿冒供應商的釣魚郵件，信中附有「最新報價單」連結，員工因缺乏辨識能力而點擊，帳號密碼當場被側錄
- 公司遭勒索攻擊後，現場無人知道該通報誰、如何隔離設備，各部門各自處理
- 某個常用軟體爆出重大漏洞，全球企業緊急修補，但公司因未訂閱 TWCERT/CC 情資來源毫不知情

➔駭客可冒名向客戶發送竄改匯款帳號的付款通知，造成客戶匯款至詐騙帳戶，公司面臨損失與商譽危機

➔災情從一台電腦擴散全公司，並因超過個資外洩通報時限，導致裁罰

➔駭客利用漏洞潛伏數週，竊取客戶資料與營業機密，發現時損害已難以挽回

如何應用

- ✓ 每季至少辦理一次資安意識宣導，涵蓋最新釣魚郵件、AI 詐騙與商務詐騙案例
- ✓ 建立一頁式「資安事件應變卡」：發現異常→立即斷網→通報窗口→保留證據
- ✓ 制定「可疑郵件通報 SOP」：員工發現異常郵件，轉寄指定資安信箱由專人判讀
- ✓ 至 TWCERT/CC 官網免費註冊，訂閱電子報接收重大漏洞與攻擊警報
- ✓ 建立「情資→行動」流程：收到漏洞警報→確認公司是否使用→48 小時內完成修補或緩解

威脅案例分析>_缺乏資安事件應變計畫

◆ 勒索軟體週五深夜發動，晚一點處理的代價，是整間公司的資料 (>室內設計公司)

某室內設計公司設計師週五深夜遠端趕圖時，發現檔案伺服器無法存取且桌面跳出勒索訊息，立刻通知老闆，老闆認為「只是中毒」，決定週一再處理。整個週末勒索軟體持續擴散，逐一加密內網中的電腦與 NAS。週一全員開機後，五年份的設計圖、客戶合約、報價單全數被鎖，**資安公司表示若當晚立即斷電隔離可保住七成資料，但拖了兩天已無法**。

> 資料損失 | 五年份專案檔案、設計圖與客戶合約全數加密無法復原

> 客戶違約 | 三個進行中的裝修案無法如期交圖，遭客戶求償違約金

> 根本原因 | 無應變計畫概念，關鍵 48 小時決策錯誤將「可控事件」拖成「全面災難」

企業資安事件應變處理指南 https://www.twcert.org.tw/tw/lp-160-1.html

防護案例分析>_ 網路釣魚攻擊

◆ 財務收到「供應商換帳號」E-Mail，一通電話擋下百萬詐騙(> 批發零售業)

某貿易公司財務人員收到供應商來信，表示因銀行整併需變更收款帳號，要求儘速匯款。郵件格式、簽名檔與承辦人名字都與過往一致，僅寄件地址多了一個不起眼的字母。**財務人員依公司規定「匯款帳號變更一律電話確認」，致電供應商後發現對方從未發出該信，立即通報 IT 封鎖該地址並全公司警示，成功在匯款前攔截詐騙**。事後追查發現，駭客已潛伏供應商信箱一個月，監看往來郵件等待下手時機。

> 預防成本：內部 SOP+每季模擬社交工程，年度成本近乎為零 | 成功攔截百萬詐騙匯款

> 守護價值：建立供應商穩固關係，反向協助供應商信箱遭駭，強化雙方資安防線

中小企業資安教育訓練影片 https://www.smelearning.org.tw/class.php?course=18442

附件一、中小企業基本資安防護自檢表

項次	評估項目	評估結果	
		是	否
一	**帳號管理**		
1	設定長、複雜且難以破解的密碼（密碼長度至少 15 碼）	☐	☐
2	使用密碼管理工具或啟用臉部等生物特徵等二階段驗證	☐	☐
3	確保每個使用者獨立創建帳號及密碼，並僅開設其工作權責所需之權限	☐	☐
4	禁止使用共用帳號，並確保人員或業務異動時，隨之調整帳號權限	☐	☐
二	**設備和資料管理**		
1	資通訊設備的作業系統和應用程式等軟體開啟自動更新並為最新版本	☐	☐
2	安裝防毒軟體，定期更新病毒碼並掃描系統	☐	☐
3	在出售或處置企業設備之前，執行原廠重置	☐	☐
4	設定設備在短暫不活動後自動鎖定或登出，防止未經授權之操作	☐	☐
5	物聯網設備於啟用時立即修改預設密碼，並確認設備連線必要性	☐	☐
6	以「3-2-1 原則」備份公司資料，並定期執行備份演練（測試和恢復）計畫	☐	☐
7	建立全設備資產清冊：納管型號、系統與維運負責人	☐	☐
三	**資安意識培訓**		
1	定期舉辦資安教育訓練課程，宣導常見資安攻擊態樣及新型詐騙，建立良好使用習慣	☐	☐
2	確保員工與合作夥伴了解保密義務並遵守相關規則，防止公司營運機密或個資外洩	☐	☐
3	確保使用雲端服務或其他外部資通訊服務時，已充分了解其安全性和可靠性	☐	☐
4	公司具備資安事件應變計畫，並確保每個員工了解相關規範與流程	☐	☐
5	加入台灣電腦網路危機處理暨協調中心 TWCERT/CC，獲取最新資安情資	☐	☐

附件二、中小企業資安參考資料資源區

中小企業網路大學校「資安刊物」參考
https://www.smelearning.org.tw/publication.php

勒索軟體防護指南 TWCERT/CC
https://www.twcert.org.tw/tw/cp-14-4843-7060c-1.html

國家資通安全研究院推廣資源
https://s.moda.gov.tw/8WPGTuqkjD6m

企業資安事件應變處理指南
https://www.twcert.org.tw/tw/lp-160-1.html

中小企業資安教育訓練影片
https://www.smelearning.org.tw/class.php?course=18442