資安風險管理—淺談攻擊表面管理

蔡永信

中華民國 113 年 6 月

作者任職於中央銀行資訊處，本文內容純屬個人意見，與服務單位無關，如有錯誤概由作者負責。

摘 要

由於科技發展日新月異以及全球性的加速推動數位轉型，相關科技之應用領域隨之擴展，企業或組織遭受惡意程式與駭客攻擊的範圍持續擴大，增加組織的攻擊表面。近期越趨嚴峻的地緣政治衝突所引發的資訊戰，駭客入侵的動機與意圖複雜化，以往被認為較不具備攻擊價值的企業與組織，也成為駭客組織攻擊的目標，當前的資安風險管理確實更加關鍵，也較以往複雜。

攻擊表面管理(Attack Surface Management, ASM)旨在全面了解和管理組織的攻擊表面，從而更有針對性地應對潛在的威脅。本文將探討攻擊表面管理的概念、建議實施作法，以及未來發展趨勢，以提供在複雜資安環境中保護資訊資產的策略與方法。

攻擊表面管理亦是一個持續的風險管理過程，幫助識別、評估和管理數位資產暴露於潛在威脅的風險，並透過持續監控和改進，保持最小化的攻擊面，以降低被攻擊的風險，其主要功能包括資產發現、資產映射、漏洞評估、風險分析、漏洞修補與持續監控。

攻擊表面評估技術包含資產發現、資產映射、漏洞評估及風險分析，其能幫助達到攻擊表面可視化，相關工具及技術可分為外部攻擊面管理、數位風險保護服務與網路資產攻擊面管理 3 大類。而實施一個持續威脅暴露管理框架，則有助於管理更廣泛的風險。

攻擊表面管理的實施需要一個具系統性且有計劃的方法，建議作法包括資產管理、攻擊媒介分析、漏洞掃描和滲透測試、監控和評估風險以及減少攻擊表面。透過持續不斷地優化實施作法，能全面而有效地降低攻擊表面，提高整體資訊安全水準。

攻擊表面管理是現代資安管理不可或缺的元素，透過資產管理、攻擊媒介分析、漏洞掃描和測試、監控與評估風險以及降低攻擊面的方法，組織能夠更全面地了解自己的資安狀態並有效應對威脅。然而，攻擊表面管理同時也面臨組織規模和複雜性增加、技術和威脅的快速變化、以及組織文化和人員培訓的挑戰。

預期未來攻擊表面管理將朝著自動化和智慧化的方向發展，並與其他管理措施進行更深入的整合，資安解決方案將更加注重預測性分析，及對新興技術的風險進行更全面的評估。總之，攻擊表面管理不僅是一種資安措施，更是保護資訊資產的重要策略，值得各界持續投注心力發展。

目次

壹、前言

隨著科技發展日新月異以及全球性的加速推動數位轉型，企業或組織的數位資產，如網站及其內容、程式碼、電子文件、雲端服務帳號及其資料等(葉慶元等(民 107))，伴隨著雲端運算、物聯網、行動應用程式等應用領域的擴展，不僅為企業帶來了更多商機，也使得企業或組織遭受惡意程式與駭客攻擊的範圍持續擴大，增加組織的攻擊表面。

此外，近期越趨嚴峻的地緣政治衝突所引發的資訊戰，讓駭客入侵的動機與意圖複雜化，使得以往被認為較不具備攻擊價值的企業與組織，如中小企業等也成為駭客組織攻擊的目標(資安人編輯部(2021 年 10 月 19 日))。由此可知當前的資安風險管理確實更加關鍵，也較以往複雜。

一、台灣上市櫃公司的資安態勢

台灣身處於 AI 科技與地緣政治的中心，資安攻擊事件數量自然是不容小覷，回顧 2023 年台灣上市櫃公司的資安態勢(Security Posture)，可發現至少有 23 起資安事件重大訊息發布於證交所與櫃買中心網站，比起 2021 年與 2022 年有明顯增加，其公告內容包含網路攻擊、個資及資料外洩等相關事件，受害產業涵蓋科技業、電子零組件與多個傳統產業，中小企業也成為攻擊目標(羅正漢(2024 年 3 月 8 日))。

今年 1 至 6 月，除了 3 月份，其餘月份至少有 3 至 6 起資安事件重大訊息公告(如圖 1 所示)，顯示台灣上市櫃企業受到駭客入侵威脅的態勢，比起過去更為嚴峻。細分這些受害公司的產業類型，可以發現科技業、電子零組件業的資安事件公告數依然佔前 2 名，而已發布資安事件公告的產業類別涵蓋面較去年更廣(如表 1 所示)。

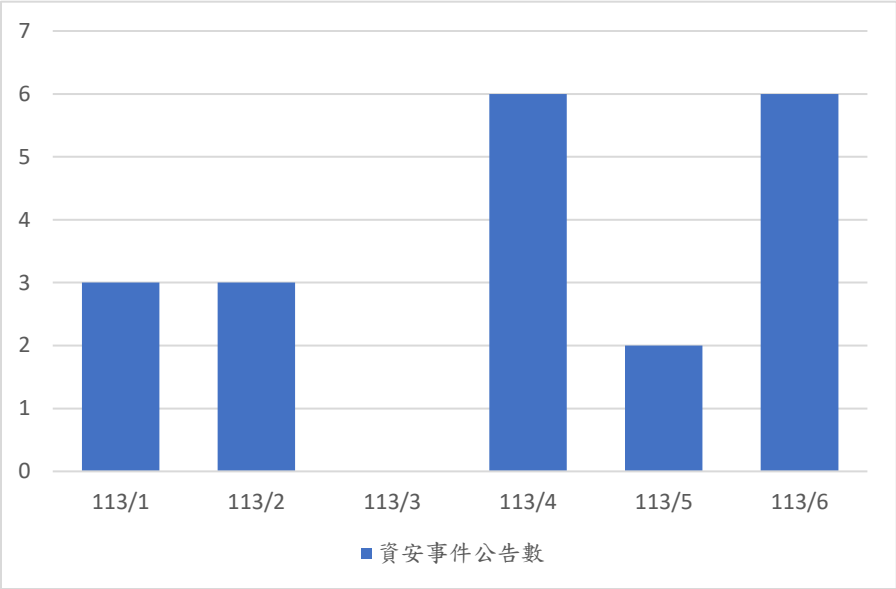

圖 1—2024 年 1 至 6 月台灣上市櫃公司公告資安事件趨勢

產業類別	資安事件公告數
半導體業	4
電子零組件業	2
生技醫療業	2
電機機械	1
運動休閒	1
化學工業	1
觀光餐旅	1
食品工業	1
塑膠工業	1
光電業	1
航運業	1
金融業	1
數位雲端	1
電腦及周邊設備業	1

表 1— 2024 年 1 至 6 月，台灣上市櫃公司依產業別的資安事件公告數
(資料來源：公開資訊觀測站)

由前述可知，台灣上市櫃公司面臨越來越嚴峻的資安威脅，資安公司趨勢科技也指出中小企業正受到勒索病毒攻擊的威脅(羅正漢(2024 年 3 月 8 日))。不只台灣，美國的關鍵基礎設施亦遭到駭客攻擊，攻擊範圍涵蓋電信、能源、水資源等領域，共有 23 家相關領域的廠商成為攻擊目標(FBI (2024))，這些事件凸顯資安在當前數位化時代的重要性，以及需要持續加強網路安全防護措施的必要性。

二、資安管理新兵器

傳統上資安防禦主要集中在防火牆、入侵偵測系統(Intrusion-Detection System, IDS)和防病毒軟體等技術，但這些傳統手段仍無法全面深入地解決現代資安挑戰，應對這樣日益複雜的資安威脅環境，攻擊表面管理(Attack Surface Management, ASM)逐漸嶄露頭角，成為保護資訊資產的關鍵一環。

攻擊表面管理，作為資安管理的新兵器，旨在全面了解和管理組織的攻擊表面，從而更有針對性地應對潛在的威脅。本文將探討攻擊表面管理的概念、建議實施作法、以及未來發展趨勢，以提供在複雜資安環境中保護資訊資產的策略與方法。

貳、攻擊表面管理概述

《孫子兵法》有云「知己知彼，百戰不殆」，乃強調在戰爭中，了解自己和了解對手的重要性，這恰好說明了攻擊表面管理的核心精神，它們之間的關聯在於攻擊表面管理中，「知己」即是了解組織自身的數位資產，包括其功能、風險和漏洞，透過持續監控和評估每個暴露在外的資產，以掌握受攻擊面。

而所謂的「知彼」即是了解潛在駭客可能利用的漏洞和威脅，我們知道駭客總是不斷掃描攻擊目標暴露在外的資產，以便趁虛而入，因此，攻擊表面管理強調透過主動搜尋駭客可能發現和利用的威脅，將網路安全保護擴展到傳統邊界之外。

由此可知，攻擊表面管理和「知己知彼」原則都強調識別、評估和持續監控潛在的安全性問題，這使得企業與組織能夠更早地針對漏洞採取行動，減少受攻擊的機會和時間，達到百戰不殆的目標。

接著，本文將解構攻擊表面，介紹駭客攻擊媒介與企業或組織的攻擊表面。

一、攻擊媒介

攻擊媒介(Attack Vector)指的是駭客用來入侵或滲透受害者數位資產的方法或工具(如圖 2 所示)，因此，攻擊媒介是駭客進行非法存取的途徑，任何允

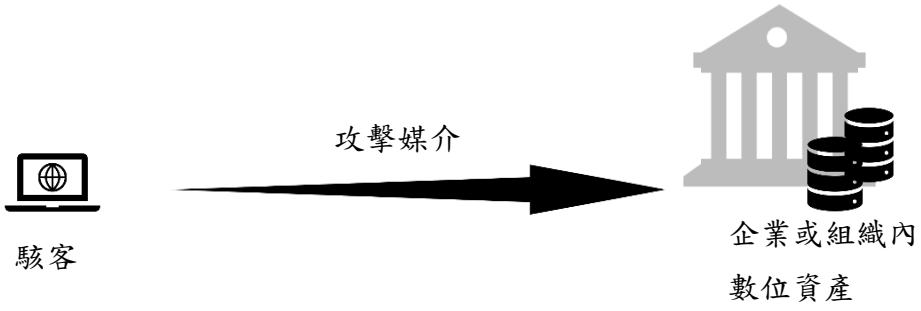

圖 2 攻擊媒介示意圖

許資料輸入到應用程式或傳輸進網路的進入點都是可能的攻擊媒介，下列是常見的攻擊媒介：

- 社交工程攻擊：利用人類心理，誘使個人透露敏感資訊或執行危害安全的操作。

●帳號密碼竊取：駭客竊取帳號密碼，以獲得其未經授權的存取權限。

●漏洞弱點利用：駭客利用軟體漏洞(如未更新的系統)來滲透網絡。

●內部人攻擊：來自企業或組織內部的攻擊，通常是不滿的員工或供應商所為。

●惡意軟體：感染系統的惡意軟體(例如特洛伊木馬病毒、勒索軟體)。

●釣魚郵件：詐欺的電子郵件，誘使收件人透露敏感資訊。

●水坑式攻擊：瀏覽被入侵的網站時，自動下載惡意程式。

●實體攻擊：實際上獲得存取權限(例如竊取筆記本電腦)，以危害安全。

●供應鏈攻擊：透過第三方供應商，以滲透目標企業或組織。

●零時差漏洞利用：在漏洞修補釋出之前，利用該漏洞進行攻擊。

二、攻擊表面

根據美國國家標準與技術研究院(National Institute of Standards and Technology, NIST)發布的資訊系統安全文件(CSRC Content Editor. (n.d.))的定義，攻擊表面(Attack Surface)是指系統、系統元件(System Component/Element)或環境(Environment)邊界上的一組侵入點(即一組攻擊媒介組合而成的表面，如圖 3 所示)，駭客可在這些攻擊面嘗試進入、造成影響與竊取資料，換言之，攻擊表面係指企業或組織網路內所有可能被駭客用來實施入侵的入口或攻擊媒介。

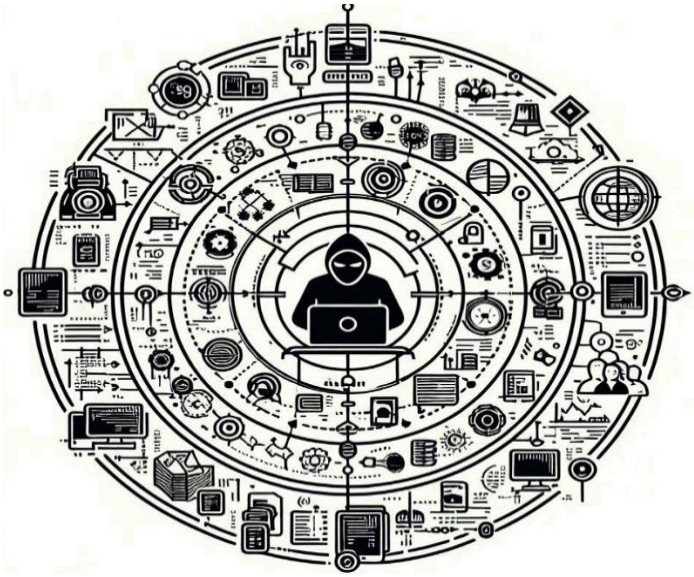

圖 3 駭客攻擊表面示意圖。
（來源：Bing Image Creator）

而實務上，駭客可利用安全漏洞或使用社交工程技術來獲得系統存取權限，入侵企業或組織內部重要資產。美國知名網路安全公司 CrowdStrike 將攻擊表面分為 3 個基本類型(Rona Kedmi. (2022))：

(一)數位攻擊表面

企業或組織的整個網路和軟體環境皆屬此類，如應用程式、程式碼、通訊埠、登入/登出點、以及未經授權使用的影子 IT(Shadow IT)。

(二)實體攻擊表面

企業或組織所有端點設備，如桌上型電腦、筆記型電腦、行動裝置和 USB 孔等駭客可以實際接觸的端點設備。這個攻擊表面還包含隨意丟棄的具敏感資料之硬體，以及實體入侵。

(三)社交工程攻擊表面

社交工程攻擊利用人性的弱點攻擊企業或組織，常見的攻擊類型包括魚叉式網路釣魚、假託(pretexting)和其他用於誘騙個人提供敏感資訊、存取權限的操縱技術。

三、攻擊表面管理

Gartner 的研究報告(Mitchell Schneider, Pete Shoard and John Watts. (2024))提到，隨著數位化轉型的加速，企業或組織的網路攻擊面變得越來越複雜和分散，攻擊表面管理已經成為現代網路安全管理策略中的核心元素。攻擊表面管理亦是一個持續的風險管理過程，幫助識別、評估和管理數位資產暴露於潛在威脅的風險，並透過持續監控和改進，保持最小化的攻擊面，以降低被攻擊的風險。

從功能面來看，攻擊表面管理是一組流程、技術和管理服務，用於識別、監控和減少攻擊表面，其主要功能包括(Pete Shoard (2021)、Rona Kedmi (2022)、IBM (n.d.)與 Brenda Gratas (2023))：

(一)資產發現(Asset Discovery)

識別所有企業或組織擁有的資產，包括網路基礎設施、軟硬體、資料庫、雲端服務、IP 位址和網域名稱等。

(二)資產映射(Asset Mapping)

建立資產之間的拓譜關係，識別駭客可能利用的所有可能的存取資產途徑，包括內部與外部的數位資產，並識別出所有可能攻擊媒介。

(三)漏洞評估(Vulnerability Assessment)

在映射出攻擊表面之後，資安團隊進行漏洞評估，以識別每個資產的安全漏洞和弱點。

(四)風險分析(Risk Analysis)

識別漏洞後，資安團隊進行風險分析，將發現的資產和漏洞放入業務和技術環境中進行情境化(Contextualization)分析，了解它們的重要性和可能衝擊，以確定成功攻擊的可能性和潛在影響。

(五)漏洞修補(Remediation)

根據風險分析的結果，安全團隊啟動修復活動，以解決識別出的漏洞，減少風險。

(六)持續監控(Continuous Monitoring)

持續監控資產和系統的安全狀況，及時發現新的漏洞和安全威脅。

上述這些步驟構成了一個全面的攻擊面管理過程，能幫助組織主動識別和減少其攻擊面，提高整體安全性。主要過程可分為攻擊表面評估(Attack Surface Assessment)(發現、映射、評估、風險分析)與管理(修補與監控)2 大類。

四、攻擊表面可視化

上一節提到的資產發現、資產映射、漏洞評估、風險分析等攻擊表面評估技術，有助於達到攻擊表面可視化(Visualization)與了解資產對駭客的吸引程度(Attractiveness)。Gartner 研究報告(Mitchell Schneider, Pete Shoard and John Watts (2024))將攻擊表面評估技術工具或服務分為以下 3 大類：

(一)外部攻擊面管理(External Attack Surface Management, EASM)

連網的伺服器、公有雲服務以及可能被駭客利用的第三方合作夥伴軟體程式，這些資產若是組態設定錯誤或有漏洞，極有可能形成被駭客利用的攻擊表面，外部攻擊面管理這項解決方案有助於發現對網際網路開放的資產和系統，或暴露於網際網路的相關資產所形成的攻擊表面。

(二)數位風險保護服務(Digital Risk Protection Service, DRPS)

本項解決方案提供對數位環境的全面監控服務，支持安全決策和戰略制定，如對網路、社交媒體、暗網(Dark Web)和深網(Deep Web)的監控，保護組織的品牌和聲譽，防止冒名頂替和欺詐活動，預防和減輕資料洩露風險，保護敏感信息，以及提供高質量的威脅情報等。

(三)網路資產攻擊面管理(Cyber Asset Attack Surface Management, CAASM)

透過對現有資安管理工具的資訊整合集中化和 API 自動化方式，提供對所有網路資產(內部和外部)的完整視角，藉由查詢整合後的資訊，識別出資安暴險範圍和資安管控缺口，幫助資安團隊克服資產可見性和風險暴露的挑戰。

五、持續威脅暴露管理

在 Gartner 研究報告(Jeremy D'Hoinne, Pete Shoard and Mitchell Schneider. (2022))中，更近一步地表示實施一個持續威脅暴露管理(Continuous Threat Exposure Management, CTEM)框架，而非僅是以技術為中心的攻擊面和漏洞評估，有助於管理更廣泛的風險。持續威脅暴露管理是一個整合的、循環的流程框架，旨在持續評估和改進企業的安全態勢(Security Posture)。該報告強調在進行風險自評時，常常因為使用不切實際的、孤立的、或工具導向的方

法，而無法有效降低威脅暴露(Threat Exposure)；而持續威脅暴露管理框架(如表 2 所示)主要由下列 3 個元件所構成：

(一)攻擊表面管理

透過前一節提到的 EASM、DRPS 與 CAASM 工具或服務，從駭客的角度，描繪出組織呈現的攻擊表面與數位風險樣貌。

(二)弱點評估

曝險管理		
攻擊表面	弱點	資安態勢驗證
內部	處理的優先順序	針對性
外部	弱點分類	綜合性
數位風險	弱點意識	合規性

表 2 持續威脅暴露管理框架

盤點資產，並分析其相關的弱點與組態設定，評估相關漏洞是否容易遭受駭客利用。

(三)資安態視驗證

透過滲透與攻擊模擬工具(Breach and Attack Simulation)或自動化滲透工具(Automated Penetration Testing)，驗證 IT 基礎設施在遭受駭客攻擊時，企業所部署的防禦措施或工具是否能有效阻擋攻擊，

透過上述 3 個主要元件建構行動專案，可以建立起一個全面且有效的威脅暴露管理框架，最大限度地減少安全風險並提升整體安全態勢。

參、攻擊表面管理建議作法

一、實施作法

攻擊表面管理的實施需要一個具系統性且有計劃的方法，以確保有效地降低資安風險，以下是主要實施的建議作法：

(一)資產管理

首先，資產管理是攻擊表面管理的基石，企業或組織必須盤點和了解其所有的資產，如硬體、軟體、資料和人員等，建立一個詳盡的資產清單，並將資產進行分類並評估其價值，此步驟有助於全面了解攻擊表面的範圍，從而能夠針對性地制定後續資安管理策略。

此外，資產管理也須確保有適當的資產保護措施，如加密、身分驗證和存取控制等。這有助於減少機敏資訊外洩的風險，確保資產在整個生命週期中都得到適當的保護。

(二)攻擊媒介分析

攻擊媒介分析是透過詳細研究外部和內部的威脅，以理解駭客可能使用的路徑和手法，外部攻擊媒介包含惡意程式、網站攻擊和入侵等，而內部攻擊媒介則涵蓋員工疏忽、內部惡意行為和資料外洩等。

透過攻擊媒介分析，可確保資安防禦策略更具針對性。舉例來說，如果發現外部攻擊媒介主要來自特定的入口點，可以加強該入口點的安全措施，或者實施員工的安全意識以減少內部攻擊發生的可能性。

(三)漏洞掃描和滲透測試

漏洞掃描和測試是確保資訊系統安全的關鍵步驟，藉由漏洞掃描工具，可以識別系統中可能存在的漏洞和弱點，另外，滲透測試則是模擬真實攻擊，試圖進一步測試系統的抵禦能力。

此步驟的目的是及時發現和修補漏洞弱點，可減少駭客利用系統漏洞的可能性；漏洞掃描和滲透測試需要定期進行，以確保系統的安全性始終保持在最佳狀態。

(四)監控和評估風險

監控和評估風險是持續改進資安態勢的重要環節，因此需要建立持續監控機制，以便能夠迅速發現任何異常組態設定或漏洞。持續監控機制包含持續攻擊表面評估，並整合現有的入侵偵測系統、安全資訊和事件管理（Security Information and Event Management, SIEM）等資安工具，提升對新威脅風險的重新評估、採取應對行動的能力。這種持續的監控和評估對於保持資安防禦措施有效性至關重要。

(五)減少攻擊表面

降低攻擊面是攻擊表面管理的核心目標之一，透過修補漏洞、強化安全組態設定、定期更新系統和應用程式，來減少駭客利用的機會。此外，員工培訓與教育也是降低內部攻擊面的重要手段，提高員工對安全風險的認識，使其能夠識別和防範潛在的威脅。

透過持續不斷地優化上述實施作法，能夠全面而有效地降低攻擊表面，進而提高整體資訊安全水準。

二、技術供應商

俗語有云，工欲善其事，必先利其器，優良的服務與技術供應廠商，將有利於達成攻擊表面管理的目標。綜觀目前市面上攻擊表面管理相關服務與技術工具的主要供應商和其提供功能(Timonera, K. (2024, June 4))，在此列舉如下：

- CyCognito：擅長發現攻擊媒介。
- Google Cloud Security by Mandiant：用於識別和管理外部攻擊表面。
- Palo Alto Cortex Xpanse：持續監控和管理攻擊表面。
- Microsoft Defender：外部攻擊表面防禦工具。
- CrowdStrike Falcon Surface：基於雲端服務的攻擊表面管理解決方案。
- Tenable：用於外部攻擊表面管理。
- IBM Randori：用於攻擊表面模擬和測試。

下一章節將探討管理攻擊表面的挑戰和未來發展趨勢，以幫助企業或組織更好地應對不斷變化的資安環境。

肆、挑戰和未來發展

攻擊表面管理雖然在資安管理發揮重要作用，但同時也面臨一系列挑戰，了解這些挑戰並探討未來發展趨勢，對於提升攻擊表面管理的效能尤為重要。

一、挑戰來源

(一)組織規模和複雜性的增加

隨著企業或組織的擴張，其資訊環境變得更加複雜，攻擊表面也會更大，比如在多雲環境、微服務架構和跨平台應用程式的混合應用場景下，攻擊表面的管理變得更為龐雜而困難。因此，攻擊表面管理需要不斷適應不同的環境，這將對資安團隊造成更大的負擔。

(二)威脅和攻擊技術的快速變化

駭客總是在尋找新的漏洞和弱點，因此威脅類型和攻擊技術也不斷演進。攻擊表面管理需要能夠及時跟上這些演化速度，否則可能無法應對新型的攻擊手法，因此攻擊表面管理工具和流程需要不斷地升級和優化。

(三)組織文化和人員培訓的挑戰

攻擊表面管理實施的成功不僅僅依賴於技術工具，還需要組織文化的支持和員工的主動參與。所以，需要建立一種具資安意識的組織文化，並確保員工具備足夠的安全知識。這需要進行定期的培訓和宣導活動，以提高組織內每個成員，尤其是非資安團隊成員對資安重要性的認識。

二、未來發展趨勢

(一)自動化和智慧化的發展

資安公司 Palo Alto Networks 發布的 2023 年攻擊表面威脅報告(Unit 42 (2023))提到攻擊表面管理的問題，其關鍵在缺乏全面能見度，因此，未來隨著技術的進步，預期攻擊表面管理將更加注重自動化和智慧化，以取得更全面性的攻擊表面可視性。自動化可以加速攻擊表面的評估和修補過程，可以

更迅速地回應新的威脅。智慧化則將透過機器學習和人工智慧，更有效地識別異常行為和模式，提高對未知威脅的檢測能力。

(二)與其他資安管理措施的整合

攻擊表面管理不應該被視為孤立的資安管理措施，而應該與其他相關的資安控制和實作進行整合。例如，將攻擊表面管理與漏洞管理、入侵偵測系統、SIEM 等整合，形成一個協同作戰的資安生態系統，有助於提高整體資安防禦的協同效應，能夠更全面地應對威脅。

(三)面向未來的資安策略和解決方案

未來的資安策略需要更加關注未來，不僅僅應對當前的威脅，還要能夠應對即將出現的風險，包括對新興技術(如物聯網、區塊鏈等)的風險進行更全面的評估，以及對新興攻擊手法的應對策略。

隨著人工智慧的快速發展，未來的資安解決方案可能更加注重預測性分析，透過大數據和人工智慧分析，預測和阻止攻擊的發生，這樣的解決方案將能夠更早地識別和應對新型的威脅，提前阻斷駭客的行動。

伍、結語

攻擊表面管理是現代資安管理不可或缺的元素，透過資產管理、攻擊媒介分析、漏洞掃描和測試、監控與評估風險以及降低攻擊面的方法，企業或組織能夠更全面地了解自己的資安狀態並有效應對威脅。然而，攻擊表面管理同時也面臨組織規模和複雜性增加、技術和威脅的快速變化、以及組織文化和人員培訓的挑戰。

預期未來攻擊表面管理將朝著自動化和智慧化的方向發展，並與其他管理措施進行更深入的整合，資安解決方案將更加注重預測性分析，和對新興技術的風險進行更全面的評估。總之，攻擊表面管理不僅是一種資安措施，更是保護資訊資產的重要策略，值得各界持續投注心力發展。

參考文獻

資安人編輯部(2021 年 10 月 19 日)。超過六成被駭台灣中小企業遺失客戶數據，修復是大挑戰。資安人。https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=9522

葉慶元、游成淵、林怡蒼、謝時峰、易欣樸、鄭雅玲、張肇虔、陳芊汝(民 107)。數位資產與數位遺產法制之研究。國家發展委員會 106 年度計畫期末報告(計畫案號：ndc106002)，未出版。

羅正漢(2024 年 3 月 8 日)。【【2023 年有 23 起資安事件重大訊息】上市櫃公司屢遭網路攻擊，中小企業災情大增。IThome。https://www.ithome.com.tw/news/161666。

FBI. (2024). Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says. Retrieved from https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says

CSRC Content Editor. (n.d.). attack surface - Glossary | CSRC. Retrieved from https://csrc.nist.gov/glossary/term/attack_surface

Rona Kedmi. (2022). What is an attack surface. Retrieved from https://www.crowdstrike.com/cybersecurity-101/attack-surface-management/.

Mitchell Schneider, Pete Shoard and John Watts. (2024). Innovation Insight: Attack Surface Management. Gartner Research.

Pete Shoard. (2021). Hype Cycle for Security Operations. Gartner Research.

Rona Kedmi. (2022). Attack surface management. Retrieved from https://www.crowdstrike.com/cybersecurity-101/attack-surface-management/.

IBM. (n.d.). What is attack surface management. Retrieved from https://www.ibm.com/topics/attack-surface-management#:~:text=Attack%20surface%20management%20%28ASM%29%20is%20the%20continuous%20discovery%2C,vectors%20that%20make%20up%20an%20organization%E2%80%99s%20attack%20surface.

Brenda Gratas. (2023). Understanding Attack Surface Analysis: Its Importance and Strategies. Retrieved from https://blog.invgate.com/attack-surface-analysis.

Mitchell Schneider, Pete Shoard and John Watts. (2024). Innovation Insight: Attack Surface Management. Gartner Research.

Jeremy D'Hoinne, Pete Shoard and Mitchell Schneider. (2022). Implement a Continuous Threat Exposure Management (CTEM) Program. Retrieved from https://www.tenable.com/analyst-research/2022-gartner-exposure-management-report.

Timonera, K. (2024, June 4). 7 Best Attack Surface Management Software for 2024. Retrieved from https://www.esecurityplanet.com/networks/attack-surface-management-tools/

Unit 42. (2023). Informe de Amenazas de La Superficie de Ataque. Retrieved from https://www.paloaltonetworks.tw/resources/research/2023-unit-42-attack-surface-threat-report