超前部署零信任 供應鏈安全成顯學

台灣亞太產業分析專業協進會 105 年認證產業顧問 童啟晟

萬物聯網，雖深化產業間的鏈結，但駭客攻擊的型態亦從單點的風險變成整個面的威脅，各行各業皆有可能成為目標，從油管系統癱瘓，到電腦大廠資料外洩、科技集團遭病毒攻擊，為了強化自身競爭力，維護信譽，產業對資安資源重視與經費配置逐年攀升，除積極採取新興技術應用在資安防護對策上，對一切存疑，包含外包廠商、上下游合作夥伴等，加強端點間的身分認證，確保存取安全後才給予連線，多方部署零信任機制，在疫情間維持生產力的同時，也不放過任何縫隙，打造一個安全的供應鏈機制。

而隨著疫情、5G、AIoT 等趨勢浪潮，對產業所造成衝擊的新常態（New Normal）如宅經濟、宅辦公，更驅動了國際大廠在零信任架構解決方案（端點、網路、人員、資料）的超前部署，混合辦公、萬物聯網造成企業遭受攻擊端點的增加，網路安全的複雜性前所未見，過去「阻絕於境外、管控於境內」的數位邊界逐漸模糊，企業必須提升資安防護的完整性進行布局，而建立營運永續與資安韌性，更使得資安產業的競局，從供應端到需求端在供應鏈暨生態系的生態系板塊產生的巨大變化。

一、零信任安全時代的主動式防禦機制

過去企業的傳統資訊安全架構，是以網路邊界防護為核心，但網路邊界亦因不同資安層級的網路（如企業外網如 Internet 與企業內網）連結而產生不同的防禦機制；位於資料中心內外網分界的閘道，就被認為是傳統資訊安全架構防護的重要網路邊界，藉由部署防火牆、入侵偵測、阻止「分散式阻斷服務（Distributed Denial-of-Service, DDoS）」攻擊等資安產品來達成防護效能；而來自外部的存取流量透過資安產品檢測後，轉發至資料中心內或雲端上的資源。但傳統的資安架構，在過去的確能有效的實踐安全防護的作用；可是在疫情之後的現階段，進階且高頻率的惡意攻擊不斷發生，這種傳統的資安體系的缺點逐漸顯露出來。

「零信任架構（Zero Trust Architecture, ZTA）」在 2009 年由 Forrester 的首席分析師 John Kindervag 提出的架構模型，主要指藉由持續驗證與授權建立動態存取信任，對任何未經過驗證的存取主體都不給予信任。而無論是「零信任」或「零信任架構」探討的是識別可存取資源、連線安全、存取控制、及特權存取管理等符合時下資安趨勢而受到重視。也就是說在數位服務系統的快速發展下，不論是「自攜裝置／設備（Bring Your Own Device, BYOD）」、整合內部介

接雲端服務、或是受到疫情影響而採取遠端工作等，強化邊界方法顯得格外重要；另外「身分與存取管理（Identity and Access Management, IAM）」、「資料外洩防護（Data Loss Prevention, DLP）」等識別可存取資源，並實施「多層要素認證 （Multi-Factor Authentication, MFA）」，都是企業數位服務落實零信任及零信任架構的核心重點。

二、資安風險的管理與企業營運的韌性

網路安全在經過 2020 年 COVID-19 病毒及駭客攻擊的考驗，含有復原力重建的韌性就成為 2021 年企業必須勇於面對試煉的關鍵字。所以企業正確制定資訊安全框架，當然對於解決問題是極為重大的策略，因為無論是「產業資安化」或「資安產業化」的共同目標不是避免摔倒，而是摔倒後能如何爬起來，這就是韌性。企業亦須從三個面向來因應資安風險，包括瞭解風險：藉由各項資安演練與檢測，瞭解企業資安風險與弱點；面對風險：藉由風險成因分析，建置企業完整資安防護體系；因應風險：透過資訊安全中心即時預警，縮短人工監控的時間差。再掌握威脅管理、弱點管理與災害後果管理等三要素，量身訂作與快速強化資安因應機制，包括成立資安緊急應變小組，進行資安災害緊急應變演練，訂定各項資安應變「標準作業程序（Standard Operation Procedure, SOP）」。

面對病毒的流行及擴張，很多專家常會強調平常免疫力的提升，無論是從身體、心理、財富、價值觀等方面的安心養神、韜光養晦做起。然而企業值此疫情熱燒的當下，更應該有做好防駭的許多準備，不管是從企業的體質、全體員工的資安觀念、企業的資安投資與人力招募、企業的永續發展及資安韌性等擘劃。全球供應鏈正面臨巨大的板塊位移。世界各國與主要經濟體正致力提升相關供應鏈的韌性與安全性，而疫情的演化，使得挑戰更加嚴峻。相對於企業的資安韌性的建構，不僅是將企業的資安防護不斷加強（河岸堤防的修築墊高），還得考慮當真的遭受駭客攻擊時，能做好事後的資安資源重部署與重調配，及企業營運不中斷的「可持續性」（像當堤防擋不住洪水時，沿河的居民要如何快速遷移，讓生活不因洪水而被中斷）。

三、結論

全球疫情爆發以來，網路安全的複雜性前所未見，企業面臨資安威脅的偵測與應變能力較過往大幅提升，但駭客的攻擊手法也正持續演變，企業建立營運永續與資安韌性的工作更是刻不容緩。在美中科技競局下，運用我國硬體製造的優勢，開發資安新興技術，將是開啟國際信任供應鏈金鑰的至關重要的環節。

此外，資安合規更是資通訊相關裝置設備／產品服務進入國際市場與價值的關鍵。臺灣為ICT 生產大國，在美中科技戰之際，資安能讓臺灣資通訊產品，成為安全產業供應鏈的重要一環。因此提升國內網通產品資安品質形象，建置品質好又要便宜的軟硬整合解決方案，打入國際有資安需求的產業供應鏈。

在數位轉型上，資安更是相當重要的基礎建設，在生活與經濟數位化的過程，越來越多的虛實整合，支付的數位型態又更多元，臺灣這麼多中小企業，資安的考驗，已不是單一技術的突破問題，這些部分都是產業的生態體系（Ecosystem）上，我國必須超前部署的重要切入點，而相關策略亦可從供需兩個面向，切入相關具體行動。畢竟，臺灣資安產業過往最大的問題，主要在於產業競爭力上，但無論是從「產業資安（應用需求端）化」及「資安產業（軟體供給端）化」等兩個不同的面向來看，都需要強化。

（一）透過「產業資安化」來協助製造與服務業轉型

觀測全球資安產業發展趨勢，目前已進入第五代的資安防禦階段，主要聚焦在解決 IoT 漏洞的資安破口【第一代為「防毒軟體（Antivirus）」；第二代為「防火牆（Firewall）」；第三代為「入侵防禦系統（Intrusion Prevention System）」；第四代為「惡意程式行為分析（Malware Behavior Analytic）」；第五代為「自動化滲透測試（Vulnerabilities & Exploits）」；第六代為「零信任安全（Zero Trust Security）」】。

但相關統計資料顯示，臺灣企業應用需求端，約 99%已部署防護軟體、約 99%已部署網路入侵設備、約 60%已部署「網頁應用程式防火牆（Web Application Firewall, WAF）」，但亦表示臺灣「產業資安化」的所在位置，並未及國際發展目前第五代的階段。

再加上就連眾多的臺灣科技大廠頻頻被駭，除了主觀上必須讓所有企業包括主力產業如製造與服務業，能未雨綢繆的落實資安觀念外，更要有隨時遭受攻擊的警覺。而聰明的企業是預期被駭客攻擊並制定因應計畫，被動的企業是被駭客攻擊後才訂定相應的安全計畫。讓臺灣產業的應用端做好資安這件事，已成為透過「產業資安化」來協助製造與服務業轉型的當務之急。

（二）藉由「資安產業化」來協助資服軟體產業轉型

分析全球資安市場結構，可以發現資安產品約占 48%，服務約占 52%；而其中資安產品市場中，軟體約占 79%，設備約占 20%，雲服務僅占 1%。但與全球相較，國內資安產業的硬體產值將近 60%左右，國外硬體設備僅約 20%；軟體產品與服務主力則為資料與雲端資料庫、郵件安全等，多以辨識與保護為主，威脅偵測、應變回應處理以及追蹤修復工具較少。如此的產業結構亟需翻轉調整，這當然亦是希冀在策略上能透過「資安產業化」來協助資服暨軟體產業轉型。

另一方面，我國資安產業的發展必須先篩選獨特價值，而發展臺灣資安新創就是一種從價值判斷到策略選擇的主軸。在其中一個首要的觀察指標，除了設定為未來若無形成具代表性、成功的資安新創，就表示資安產業沒有起來之外；如何對焦到臺灣整個產業環境、未來發展趨勢、產業結構調整、產業競爭力、人才供需，或是協助法制調適等指標，才能加速並深化「資安產業化」的發展。

當前美中競局下，供應鏈安全已成為臺灣資安產業發展的優勢；但資安業者規模不大，國際行銷資源薄弱；如何利用歐美對供應鏈安全要求，AIoT 資安產品需求則是重要契機；而國際資安新創解決痛點差異化的成功商模與募資能力則是我國資安新創「衡外情、量己力」之外，制定「大市場、小題目」的策略思維。乘著 AIoT 資安產品服務需求的態勢，資安新創結合 ICT 產業大廠之全球生產布局優勢，成為開啟國際信任供應鏈金鑰的隱形冠軍。

(本文作者為資策會 MIC 執行產業技術基磐研究與知識服務計畫產業分析師)

原文出處：ITIS 智網 http://www.itis.org.tw/