力阻火燒連環船！製造業「供應鏈資安」環環相扣

■文：任芷萍

照片人物：睿控網安 (TXOne Networks) 首席解決方案架構師劉大川

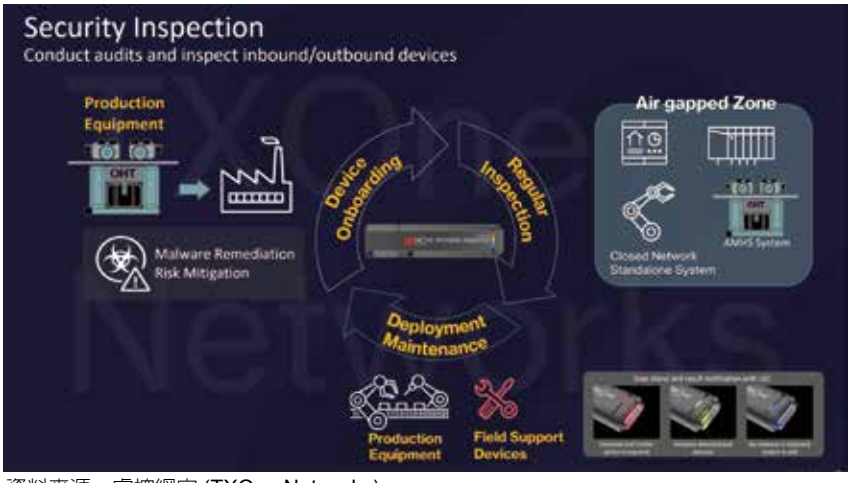
日前在《SEMICON TAIWAN 2023 國際半導體展》上，幾位熟稔智慧製造資安的專家也針對相關議題分享看法。睿控網安 (TXOne Networks) 首席解決方案架構師劉大川表示，工業資安影響最為巨大的當數供應鏈供擊，製造業資安事件有半數 (近 47%) 是因新購設備進廠前未確實完成安檢、致使自帶威脅進入場域而觸發。台積電 (TSMC) 2018 年爆發重大資安事件後，2019 年開始推動 SEMI E187 法案，它亦是首個由台灣主導之半導體產線設備資安標準規範，旨在訂立新進設備在進廠前的安檢程序和規範是否有符合資安要求。

睿控網安：生產場域網路須有「隔水艙」設計

劉大川點出這意謂：供應商在交付機台前必須把資安提到某個水準之上，這與美國去年力推的網路安全構想不謀而合。與其為待售機台外加許多資安防護，倒不如從設備設計之初就把資安納入考量，並在進廠前、例行性維修、歲修維護期間皆須做安檢，以確認任何改變、更動、移置機台的行為皆不會讓病毒有任何可趁之機。以往，在機台進廠前的掃毒健檢標準程序是：拆機殼、裝光碟機和防毒軟體，待掃描完成再移除光碟機、裝回機殼，然而麻煩的是，一旦機殼拆了後再裝回去就需重新校正，曠日廢時。

劉大川解析，一個變通方式是利用 USB 裝置進行掃毒或弱點評估，之後再出具符合 SEMI E187 的合規報告。評估要項包括：作業系統 (OS) 是否過期？機台是否存在弱點？其中有無潛藏病毒？以上規範皆須符合，且機台必須安裝防毒軟體才得以進廠。但在實務上，若考慮到機台資源有限、安裝防毒軟體恐影響效能，則至少要羅列「白名單」(Trust List)，強制二擇一；更不允許早期連登入帳號、

圖 1：新購機台設備進廠前須經安全檢查



資料來源：睿控網安 (TXOne Networks)

密碼都沒有控管，開機就能運作的情況發生。另一個由英特爾 (Intel) 主導的規範 SEMI E188 則是為減少惡意軟體傳播到製造設施、並在製造設施內傳播定義框架。

他深入剖析，SEMI E188 有兩大主要精神：首先，生產場域的網路須有「隔水艙」設計，以免不慎破了一個小洞就可能拖累整艘船沉沒；TSMC 在經歷 2018 年資安教訓後，TXOne 隨即在隔年配合 TSMC 開發「隔水艙」公共等級的防火牆。與一般防火牆最大的區別是：除了對外連網的控管外，還將工廠內的可編程邏輯控制器 (PLC) 等作業機台身分認證、讀寫權限及通訊協定列管。(參閱：《防毒如防疫，工控資安需做好區段隔離＆邊界管理》一文 http://www.compotechasia.com/a/opportunity/2021/0823/48826.html)

新購生產設備三原則：進廠安檢、端點防護、網路切割

其次是老舊弱點屏蔽問題；以前還可用事後補丁 (Patch) 處理，但自從 E187 明訂新機台掃描完、若發現重大弱點必須修復後方能進廠，此法已不可行。為周全起見，特別在正式條文之外的實務指引明訂：中階以下的設備對於低階弱點要有屏蔽及補償措施，一言以蔽之，進廠安檢、端點防護措施、網路切割 (Segmentation) 是三大原則。E187 要求的是的 baseline

圖 2：SEMI E187(白字)——Secure by Design vs. E188(黃字)——Secure by Operation

資料來源：睿控網安 (TXOne Networks)

(基本準則，至少要做到才能進廠)，在產品設計階段就要把資安思維內化到其中，例如，人機介面 (HMI) 要有帳號密碼控管、內部規格要有資安考量、資料流對驗證有無限縮、對使用者的授權……。

從生命週期的角度來看，從設備製造商的設計到客戶端進廠配置、配方、強化端點，再到後續維修，聚焦的是「Secure by Design」觀念。劉大川繼續剖析 E187 有四大構面：不能使用過期的作業系統、網路須使用加密通道、終端端點要有防護、要有稽核軌跡。E188 著重的是「Secure by Operation」，不僅網路要做 Segmentation、隔水艙，生產設備端點經過任何變更、改變、維護、升級再回到產線之前，都須再做一次掃毒，確認「Malware Free」(沒有惡意軟體、病毒)，但沒強制要安裝防毒軟體。

劉大川補充，有鑑於條文未明列時間點的定義，為免爭議，SEMI 近期即將出爐的「落地指引」檢核名單會增列時間因素，載明多久時間以內的病毒碼或掃毒程序才有效？作業系統的效期？另端點若是選擇採用但在實務上，若考慮到機台資源有限、安裝防毒軟體恐影響效能，則至少要羅列「白名單」，以預載最佳，可減少許多整合測試等不必要麻煩，並須文件告知這些防護措施不會影響機台效能。成立於 2003 年、最早投入弱點掃描、同時著墨端點資安與物聯網資安解決方案的中華龍網 (DragonSoft)，則針對「供應鏈資安與零信任」提出見解。

中華龍網：「零信任」意即永不信任、持續驗證

中華龍網總經理孫建興直言，2018 年 TSMC 機台遭到勒索病毒感染、導致營收損失新台幣 52 億元一事，確實是喚起世人對於半導體供應鏈資安重視的轉折點；去年輝達 (Nvidia) 傳出遭駭客攻擊、被竊取大量資料的消息，又突顯了網路安全 (Cybersecurity) 的迫在


照片人物：中華龍網 (DragonSoft) 總經理孫建興

眉睫。事實上不只半導體，近年頻繁遭受駭客攻擊的產業供應鏈還包括：生命科學／健康照護、汽車、消費零售和能源。當系統整合商 (SI) 把產品推向企業，客戶端未必知道背後軟、硬體供應商身分；由於當中牽涉繁多，越往供應鏈下游走、可視性越差、風險越大，越難掌握是哪一個供應環節出狀況。

孫建興指出，軟體供應鏈攻擊模式有四大類：1. 軟體供應商本身就是攻擊者；2. 軟體供應商被攻擊者所駭，其軟體產品因而被埋入惡意程式；3. 軟體供應商的產品使用含惡意程式的第三方軟體；4. 軟體供應商的產品使用含易遭駭程式漏洞的第三方軟體。毫無疑問，所謂免費的有時反而最貴，開源軟體等第三方軟體本身即蘊含高風險值；它的版本管理機制通常相對鬆散，駭客有較多機會將惡意程式或程式漏洞植入常用的開源軟體套件。有鑑於此，不同產業除了訂有相關標準加以規範外，更重要的是做到「零信任」(Zero Trust)。

孫建興解釋，所謂的「零信任」指的是：永不信任、持續驗證，旨在讓正確的身分可以存取由正確程式碼授權的正確機器，並在正確時間與情境下，存取到正確的資料。NIST (美國國家標準暨技術研究院的前身為國家標準局) 對此訂有 SP 800-207 (ZTA) 零信任架構，核心組件欲存取內、外部資源皆須從嚴經過 PKI (公開金鑰基礎建設) 數位簽章或認證等審核，且要確保機器須合規、沒有潛藏已知資安問題；與此同時，政府正力推「FIDO」(Fast IDentity Online，金融行動身分識別標準化機制) 快速認證，將分為三個階段推行：

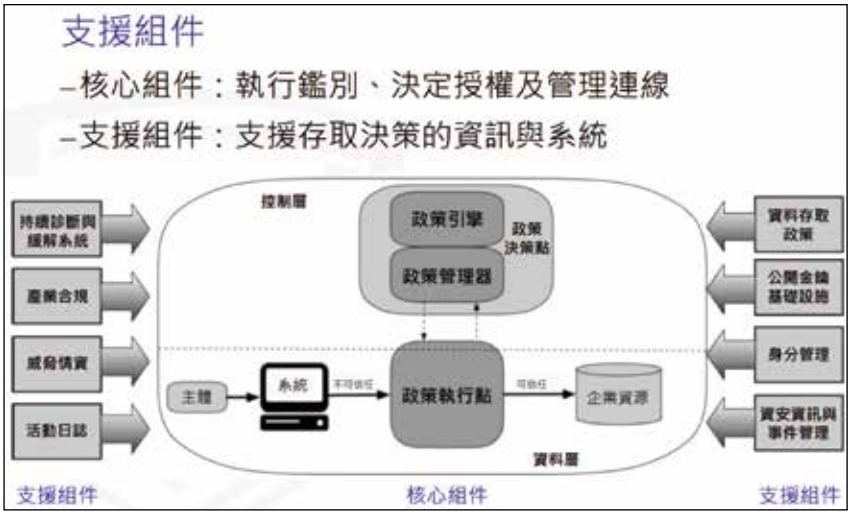
- 2022 年，身分鑑別：以生物識別鑑別器進行無密碼雙因子身分鑑別；
- 2023 年，設備鑑別：基於信任平台模組 (TPM) 之設備鑑別，並進行設備健康管理；
- 2024 年，信任推斷：依設備健康狀態、資安威脅情資及使用者情境等資訊，動態支援存取決策。

端點資安合規管理平台：以資產盤點爲基礎

「端點安全是核心，然後才有零信任和供應鏈安全可談」，孫建興強調。於是，中華龍網推出「端點資安合規管理平台」，以資產盤點為基礎，查核有無資安威脅？弱點？是否安全組態？作業系統／軟體是否合規？其中，又以下列三個面向最為關鍵：

1. 資訊資產管理 (IAM)：盤點政府／企業內部個人電腦及主機之數量、作業系統版本及配置部門等相關資訊，以利資管人員掌握場域端點及維運管理；
2. 電腦安全組態基準 (政府組態基準 GCB ／金融組態基準 FCB)：將政府／金融內部個

圖 3：NIST SP 800-207 (ZTA) 零信任架構



資料來源：中華龍網 (DragonSoft)；行政院國家資安研究院

人電腦及主機，套用符合美國 NIST 規範之一致性安全組態設定 (如：密碼長度、更新期限等) ，以降低遭駭客入侵之風險；

3. 軟體弱點管理系統 (VANS)：盤點比對政府／企業內部個人電腦及主機安裝之各類應用軟體已知的弱點或漏洞，進行修補更新，避免遭駭客利用，入侵企業網路及在內網橫向滲透。

孫建興進一步介紹 VANS 機制的目標是結合資訊資產管理與弱點管理，掌握整體風險情勢，並降低重大弱點爆發時可能造成之損害，包括：定期蒐集主機與電腦所使用之資訊資產項目及版本，建立資訊資產清冊，以達到降低風險與管控成本等目標，以及將資訊資產清單與弱點資料庫比對，以掌握所使用之資訊資產是否存在已公開揭露之弱點資訊。所謂的資訊資產涵蓋：應用軟體資產、應用框架、程式語言、應用程式中介軟體及作業系統，並揭示 TW GCB 發展規劃去年已將伺服器劃歸範疇。

他自豪地說，中華龍網不僅在 PC 端的 GCB 導入經驗豐富，伺服器的導入經驗亦優於其他廠商，且產品已經西門子 (SIEMENS) 等國際大廠認證，用戶遍及地方政府、桃園國際機場交通設施及金融證券櫃買中心，並統整中華龍網在 GCB/FCB 擁有四大優勢：

●完整售後服務：是台灣自主研發廠商，專案客製化能力強且彈性高；

●伺服器導入經驗豐富：提供逾十家客戶伺服器導入服務，例如：新北地政 (500 台以上規模)、合庫人壽、宜蘭縣政府等；

●稽核市占率最高：

◎政府體系——國內主要資安稽核廠商 (安碁、關貿、數聯、凌群、果核、漢昕)，均使用做為稽核各政府機關是否合規之工具；

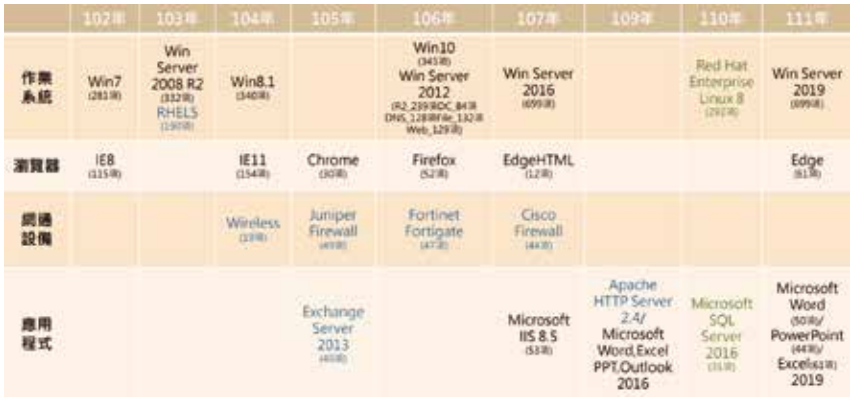
◎教育體系——為教育部 (資科司) 針對教育體系客製開發專屬稽核暨評量工具合作夥伴；

◎國防體系——為針對國防體系客製開發專屬稽核暨評量工具合作夥伴。

●Linux 稽核及導入服務：金融單位 Linux 導入服務、客製稽核工具 (用 CIS 做標準)，以及原廠服務支援。

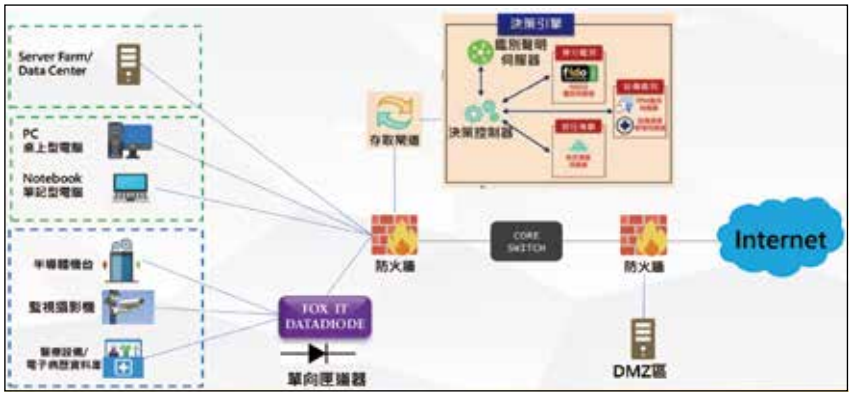
最後，他重申要打破內、外網概念，一律採「零信任」原則，即使是內部人員存取內部資訊也須經過認證，並強烈建議從 OT 場域丟出來的資料，最好走單向閘道器是最安全的方式——即使場域外有風險，也能有所緩衝、區隔；而整個 OT 環境最好維持對外封閉，不允許擅自安裝任何應用程式，將是最經濟有效的作法。更多訊息可參閱：https://www.dragonsoft.com/ 或 https://youtube.com/@dragonsoft4140?si=K6tGQ7ICux5QmQsm。CTA

圖 4：TW GCB 發展規劃



資料來源：中華龍網 (DragonSoft)

圖 5：中華龍網物聯網資安解決方案示意



資料來源：中華龍網 (DragonSoft)