經濟日報 商情 ICT趨勢

半導體產業資安風險升溫 長茂科技攜手業界強化供應鏈防護

本文共2095字

00:00

2025/03/20 17:25:50

經濟日報 林政傑

隨著全球數位化與供應鏈整合加深，半導體產業正面臨嚴峻的資安挑戰，為協助業界強化防護，新竹市企業經理協進會與台灣中小企業資訊安全協會於3月20日(四)聯合主辦「高科技產業面臨的資安挑戰與因應對策—以半導體產業為例」資安專題講座已圓滿成功。

長茂科技攜手漢翔航空工業、工研院資訊與通訊研究所、資策會資安科技研究所，聯合發表「層層隔離」技術架構理論，及資策會資安所李榮三所長蒞臨指導，提供業界高效、低成本的資安解決方案，特別針對資源有限的中小企業，透過「PC-SEC」資安系列產品，打造安全、可負擔的端點資安防護機制。

今日資安專題講座特別來賓，由左至右依序為：台灣中小企業資訊安全協會蔡英德理事長、明新科技大學呂明峯校長、新竹市企業經理協進會鄭敦仁理事長、新竹科學園區同業公會王永壯秘書長。林政傑/攝影

全球供應鏈的資安挑戰

隨著科技產業的全球化發展，半導體供應鏈涵蓋眾多供應商與合作夥伴，任何環節若出現資安漏洞，都可能成為駭客攻擊的突破點，影響企業營運甚至國家關鍵技術安全。台灣中小企業資訊安全協會名譽理事長魏得恩指出：企業需在有限資源下應對來自全球的無限攻擊，因此應建立零信任架構（Zero Trust），並透過身份驗證與存取控制來降低資安風險。

晶片與供應鏈安全的多重防護

資策會資安科技研究所技術總監張文村指出，供應鏈安全不僅關乎企業內部，也涵蓋所有合作夥伴，企業應建立供應鏈安全管理機制，以提升整體防護能力。蕭榮興主任則強調，半導體產業的核心技術-晶片若遭駭客攻擊，後果將十分嚴重，因此業界需導入安全加密通道技術(包含硬體信任根、後量子加密等)，以確保產品安全。

國際標準CMMC架構導入策略與借鏡

工研院資訊與通訊研究所技術組長卓傳育介紹SEMI E187 VoC（Verification of Compliance）驗證計畫是協助半導體廠商建立符合產業標準的資安防護策略，同時亦可提升其供應鏈內部與合作夥伴的資安透明度與合規性，降低風險並增強市場競爭力。同時，漢翔航空工業資訊處處長方一定表示，在導入CMMC（Cybersecurity Maturity Model Certification）架構的過程中，其供應鏈是採取分階段資安強化策略，在確保資安合規性的同時，並兼顧中小企業可負擔性與實際應用的需求，這一經驗對半導體供應鏈極具借鏡價值。

「層層隔離」技術架構 強化供應鏈安全

傳統資安解決方案往往成本高昂、技術門檻高，導致中小企業難以全面導入資安防護。數字嶄新有限公司總經理呂理哲表示，供應鏈企業普遍面臨資源受限、缺乏專業資安人員的挑戰，使駭客更容易利用漏洞發動攻擊。長茂科技研發的「層層隔離」技術架構，透過多層防護機制，開發出PC-SEC資安產品系列即是應用於端點設備的「微隔離」技術，即使駭客突破部分防護層，也難以進一步滲透系統。

除了端點層面的資安強化，網路層面的防護同樣關鍵。由工研院研發的「Janus自動化網路控管技術」能夠自動學習企業內部流量行為，並透過AI技術執行「自動化網段隔離」，有效阻擋未經授權的存取與橫向移動攻擊。Janus則透過動態網段劃分，讓不同設備之間形成獨立的安全區域，並根據流量異常即時調整存取規則，即使某個節點遭受攻擊，也能確保威脅不會擴散到其他區域，降低潛在資安風險，提升企業的整體網路安全性。我們希望透過PC-SEC與Janus方案，讓中小企業能獲得與大型企業同等級的資安保護，確保半導體供應鏈的安全與穩定。

數字嶄新有限公司總經理兼長茂科技資安顧問呂理哲，於講座中說明企業可以如何進行有效的資安投資。林政傑/攝影

技術創新：PC-SEC資安系列具備關鍵資安防護功能

◆身份驗證與存取控制

TP-Keep：身分驗證與密碼管理，確保安全登入

TP-Guard：零信任登入防護，僅限本人存取電腦

TP-RDP：雙因子驗證遠端桌面，防止帳密外洩導致入侵

◆資料與系統防護

TP-File：AES 256 檔案加密，防止資料被勒索或破解

TP-CFA：資料夾防護，避免惡意程式加密或竊取內容

TP-ACL：白名單管理，凍結未認證應用程式，杜絕惡意軟體

◆網路與外部裝置安全

TP-Firewall：自動學習安全 IP，防止未授權變更防火牆

TP-USBG：USB 防護，阻擋惡意 USB 裝置，防止病毒入侵

PC-SEC資安產品系列：滿足不同企業需求

長茂科技推出「PC-SEC」資安系列產品，提供三種規格，滿足不同規模企業的資安需求：

產品類別		PC-SEC	PC-SEC Pro	AD-SEC Suite	
				PC-SEC Plus	AD-SEC
適用系統		Win10/Win11家用版與專業版			Windows Server 2016 以上
AD場域適用		X	X	⊙ 受AD控制的PC	⊙
零信任身分驗證與存取控制	TP-Keep App	✓	✓	✓	✓
	TP-Guard	✓	✓	✓	✓
	TP-RDP	x	✓	✓	✓
檔案與系統安全隔離	TP-File	✓	✓	✓	✓
	TP-CFA	✓	✓	✓	✓
	TP-ACL	x	✓	x	✓
網路與裝置安全防護	TP-Firewall	x	✓	x	✓
	TP-USBG	x	✓	x	✓
適用場域/功能		一般用於無AD環境之個人用或微小企業的PC免於勒索攻擊	一般無AD環境中小企業的PC，免於勒索攻擊及抗橫向攻擊	有AD環境企業的PC，免於勒索攻擊及抗橫向攻擊	保護Windows Server免於RDP(遠端桌面)的駭客攻擊及抗橫向攻擊

長茂科技推出「PC-SEC」資安系列產品，提供三種規格，滿足不同規模企業的資安需求。長茂科技/提供

提升個人資安意識 共同守護產業安全

除了企業層面的資安防護，個人資安意識亦不容忽視。台灣中小企業資訊安全協會理事長蔡英德提醒：駭客常利用社交工程（Social Engineering）手法，如釣魚郵件或假冒訊息竊取機密資訊，因此企業員工應提高資安意識，以防成為攻擊突破點。建議企業定期進行員工資安教育訓練，並建立事件應變機制，以在資安風險發生時能迅速應對。

攜手推動產業資安發展

本次「PC-SEC抗橫向攻擊資安防護解決方案」的發表，獲得台灣科學園區科學工業同業公會、明新科技大學、資策會資安科技研究所、中華民國電腦商業同業公會全國聯合會、台灣交通大學校友總會、長茂科技、漢民科技、陽明交通大學電子物理系所/電子物理系系友會、數位科技創新發展協會、新竹市企業經理協進會雲端委員會、嶄新科技、慧鴻資訊科技、逢甲科技聯誼會等單位協辦。

未來，長茂科技仍持續致力與業界夥伴合作，提供最新資安技術與解決方案，協助半導體供應鏈強化資安防護，確保全球市場競爭優勢。