第13屆CIO價值學院第三堂課 資訊安全

資安威脅創新高 衝擊全球經濟發展

疫情重創全球，然駭客組織並沒有停止發動攻擊。根據 Google 統計每天有 1800 萬封的 COVID-19 相關的惡意程式和網路釣魚郵件，以及每天超過 2.4 億則與 COVID-19 相關的垃圾訊息。

文／林裕洋

資安向來是企業最頭痛的問題，即便斥資添購各種資安防護設備，仍然無法完全阻擋資安事件發生。尤其近年來人工智慧和機器學習等演算法日益成熟，雖然有助於企業的決策能力，但也物聯網、雲端運算、微服務等架構，均須透連網才能產生預期效益，也為資安團隊帶眾多挑戰。如在 COVID-19 疫情重創全球經濟，並使得超過1300萬人感染的狀況下，駭客組織並沒有停止發動攻擊，反而是大量假造各種與疫情相關訊息，以便達到入侵企業網路、竊取商業機密的目的。

一零四資訊科技資安品質處資安長朱建國表示，企業在仰賴資安設備協助之外，也必須強化員工安全意識，以及提高設計師的資安意識，才能從源頭降低資安事件發生。

如Google便公開宣佈安全系統已經偵測到新型態的網路垃圾郵件，如偽裝成慈善機構、非營利組織對抗 COVID-19 疫情的相關內容，或是公司主管寄給遠距工作員工的信件，甚至是醫療保健相關的疫情通知，藉此引誘人們點擊釣魚連結。根據Google統計每天有1800萬封的 COVID-19 相關的惡意程式和網路釣魚郵件，以及每天超過2.4億則與 COVID-19 相關的垃圾訊息。在此狀況之下，企業在疫情期間除維持公司正常營運下，也得兼顧惡意程式對企業帶來的嚴峻挑戰。

CIO協進會理事長盛敏成指出，日益嚴峻的資安威脅事件，對於企業有如不定時炸彈，即便平時已做好完全準備，仍然難以有效阻擋意外事件發生。在疫情指揮中心的超前部署下，台灣在對抗 COVID-19 疫情有傑出表現，多數產業都能維持正常營運，然仍然應該持續關注駭客運用此疫情發動攻擊的趨勢，才能在後疫情時代維持在市場上的競爭力。

專程到場參與此盛會的一零四資訊科技資安品質處資安長朱建國表示，企業在仰賴資安設備協助之外，也必須強化員工安全意識，以及提高設計師的資安意識，才能從源頭降低資安事件發生。

CIO協進會理事長盛敏成指出，台灣在對抗 COVID-19 疫情有傑出表現，多數產業都能維持正常營運，然仍然應該持續關注駭客運用此疫情發動攻擊的趨勢，才能在後疫情時代維持在市場上的競爭力。

勒索軟體橫行 吹起文件保護風潮

回顧2017年5月，埋伏多時的勒索軟體-Wanncry，在指定時間攻擊全球多個國家，造成前所未有的嚴重災情，並要求以比特幣支付贖金。根據統計，全球有超過150國家受害，直到2018年仍然傳出有不少國家受害，駭客組織收到贖金金額也難以估計。從此開始，勒索軟體似乎成為駭客慣用攻擊受法，如知名半導體業者也傳出遭到勒索軟體入侵，雖然僅短短停工一天，但卻造成超過數十億台幣的損失。

為此，金山軟件推出的WPS，

在主打與 MS Office 完全相容、授權費用更合理之外，也從內部安全交換、外部安全可靠等兩大面向，設計一套安全資料儲存與交換機制。在內部安全交換部分，則在WPS文件中加入內部文檔數據許可權管理體系、文檔數據加密機制、操作日誌留痕審計、保證企業內部文檔數據的轉換安全可控等功能。至於外部安全可靠機制部分，則是納入通過對文檔設置許可權、分享途徑的安全管理、洩密溯源機制的建立、實現文檔數據在對外流動上安全性的保證等機制。

TCIC環奧國際驗證公司全球營運總經理梁日誠指出，國際資安標準 ISO/IEC 27001、國際隱私資訊管理標準 ISO/IEC 27701 等，就成為時下金融科技業者積極取得合規的標準，顯見創新業者都非常注重資安問題。

金山辦公軟件台企總經理陳豪欽指出，因應時下在不同設備中讀取檔案中的需求，我們發展出以檔案為主體的雲文檔管理系統。為此，我們在雲文檔上提供文件加密，除傳輸過程有 AES-256bit 加密設計之外，還進一步推出DMS（Document Manager System）機制，提供存取、列印、浮水印等權限控管功能。這項功能提供線上預覽、共用URL連結、文檔權限控管等三大功能，以線上預覽為例，即可兼顧避免文檔下載、閱讀更便捷、本地不留痕等三大優點。

TCIC環奧國際驗證公司全球營運總經理梁日誠指出，自從歐盟新版個人資料保護法上路之後，全球企業都此法規相當關注，特別是以創新金融服務為主的金融業者。因此，國際資安標準 ISO/IEC 27001、國際隱私資訊管理標準 ISO/IEC 27701 等，就成為時下金融科技業者積極取得合規的標準，顯見創新業者都非常注重資安問題。


金山辦公軟件台企總經理陳豪欽指出，2017年5月Wanncry在指定時間攻擊全球多個國家，造成前所未有的嚴重災情，並要求以比特幣支付贖金，也吹起企業保護資料安全的概念。

整合多項資安功能 縮短挖掘威脅時間

面對日益嚴峻的資安威脅，企業被迫購買多種資安設備組成防禦網，以便抵禦來自四面八方的資安威脅。只是資安設備品牌眾多，衍生出管理上的難度，加上端點設備的資源有限，若同時安裝多套軟體，最終將影響到員工的日常工作。為此，CrowdStrike推出CrowdStrike Falcon 平臺，防毒、端點檢測和回應等三大功能，而端點設備只需要安裝25MB大小的代理程式，即可得到該業者提供的24小時威脅偵測服務服務。

根據CrowdStrike提供技術資料指出，CrowdStrike Falcon 平台最大特色，採用融合人工智慧、機器學習技術的非特徵比對手法，可針對攻擊行為進行分析，進而達到即時阻止已知和未知的威脅，保護企業免於受到各種網路攻擊的目的。特別是該公司採取獨特的雲端架

構，可提高對惡意攻擊的反應能力，企業無需另外添購軟硬體，即可使用非特徵比對技術，進而達到降低保護端點設備安全的成本。

敦陽科技資深技術經理廖盈昇指出，CrowdStrike服務的核心技術，是採用自行研發的創新技術－Threat Graph。該技術會針對位於全球各地的數百萬個CrowdStrike感應器，運用AI技術對資安事件進行關聯分析。如此一來，在最短時間察覺是否有入侵行為，並在當下立即阻斷。正因如此，在 Real-World Protection Test 公布的研究報告指出，CrowdStrike於惡意攻擊測試中，展現出100%偵測成功零誤判的成績。

台灣駭客協會HITCON顧問邱銘彰表示，過去幾年，駭客攻擊手法持續在進化中，甚至運用AI技術加速惡意程式的發展。當然，AI技術也成為資安公司防杜新型態威脅的重要工具，藉由AI演算法搭配後台運算能力，資安設備可以縮短偵測未知威脅的能力，從看似平常網路封包中，找到潛藏於其中的惡意攻擊手法。

台灣駭客協會HITCON顧問邱銘彰表示，藉由AI演算法搭配後台運算能力，資安設備可以縮短偵測未知威脅的能力。

資安威脅衝擊經濟 損失金額達6000億美元

為獲取龐大經濟利益，駭客組織從來沒有放棄過任何攻擊機會，反而積極發展新世代攻擊手法，以便趁企業疏失之際入侵。因此，根據McAfee公布調查報告指出，2017年資安事件造成全球經濟損失金額達到6000億美元，遠遠超過多數人的想像。至於資安威脅部分，依照 IT Governance 調查指出，2019年最常見5種網路攻擊手法，分別是釣魚、勒索病毒、DDoS、病毒和攻擊向量（如SQL Injection）等。

以多數人熟悉的DDoS攻擊為例，基本可分成針對基礎設施層、應用程式層等攻擊兩大類，駭客組織會在短時間內運用大量合法或偽造的封包或請求，讓目標系統無法負荷，最終出現服務被癱瘓。在兼顧攻擊效益與成本下，市面上出現脈衝式(Pulse Wave) DDoS攻擊手法，即在短短幾分鐘衝上350Gbps攻擊流量後，迅速暫停攻擊，並且採取週而復始的攻擊策略。在雲端服務領域耕耘多年的蓋亞資訊認為，雲端服務是最有效防禦DDoS攻擊的解決方案，除有彈性、高可用度之外，還具備更高規格的資料保護機制、法規遵循等，還能有效防禦DDoS攻擊。

「傳統資安防護機制是以有限資源對抗駭客的無限資源，難以展現有效的防護成果，而大型雲端供應商擁有龐大的資源，自然具備與駭客對抗的能力。」蓋亞資

敦陽科技資深技術經理廖盈昇指出，採用雲端架構的安全方案，企業無需另外添購軟硬體，即可使用非特徵比對技術，進而達到降低保護端點設備安全的成本。

訊執行長吳炳鈞解釋：「例如在抵禦DDoS部分，可運用BGP路由宣告，將攻擊流量導入雲端清洗中心，最後在將清洗後的乾淨流量，透過 GRE Tunnel 送回原本路由，所以可承受更大量的DDoS攻擊。」

行政院資安處處長簡宏偉說，根據主管機關調查2019年機關的35項實施情形中，推動資通安全管理法啟動之後，逾限且未完成率相對較高的項目，除資安專職人力、資安推動小組外，稽核相關作業亦是未完成情形較高之項目。

迎合國際趨勢 台灣資安法上路

資訊程度高低決定企業與國家的實力，台灣政府自然也積極推動數位政府，除提供民眾更便利服務之外，也致力強化台灣在世界舞台上的競爭力。因應資訊科技發展，主管機關也公布相關資安管理法規，以至於原有資安相關法規目的各異，且適用對象僅限於特定部門或事項，無法有效因應日益複雜的資安問題。

在資安等於國安的思維下，總統府已於2018年6月6日公告「資通安全管理法」，並且在2019年正式實施。該法規除規範公務機關外，亦將關鍵基礎設施提供者納入，並要求應以風險管理為核心，訂定資通安全維護計畫及通報應變辦法，並接受相關主管機關查核。此法案，除有助於落實國家資安防護策略外，也為台灣資安產業帶來新的營運商機。

行政院資安處處長簡宏偉指出，政府推動資通安全管理法的立法目的，主要目的為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益。至於規範對象，則是以對人民生活、經濟活動及公眾或國家安全有重大影響者為納管對象，如前述提到的關鍵基礎設施提供者。

該法案啟動之後，根據主管機關調查2019年機關的35項實施情形中，逾限且未完成率相對較高的項目，除資安專職人力、資安推動小組外，稽核相關作業亦是未完成情形較高之項目。至於A、B、C級公務機關資安專職人員配置及持有資通安全專業證照及資通安全職能評量證書符合情形部分，A、B級機關符合率均超過40%以上，而C級機關僅有32%左右。而在未來工作目標方面，行政院資安處將重在落實法規要求，同時全力推廣分層管理、資安意識提升、委外服務供應鏈管理等。

蓋亞資訊執行長吳炳鈞解釋，傳統資安防護機制是以有限資源對抗駭客的無限資源，難以展現有效的防護成果，而大型雲端供應商擁有龐大的資源，自然具備與駭客對抗的能力。

減輕資安長負擔 仰賴自動化工具

隨著全球對資安事件日益重視，企業、政府紛紛強化在資安防護上的投資，面對持續爆發的資安威脅事件，資安長肩膀上的責任也

持續增加，可說有做不完的代辦事項。為此，在資訊安全領域著墨極深的IBM，則有完整產品線可協助資安長快速達成辨識、回應、自動化、保護等工作，讓公司具備快速處理各種資安威脅事件的能力。

如 IBM QRadar User Behavior Analytics（UBA）可分析內部人員的使用型樣，以判斷其認證或系統是否已遭到網路罪犯的損害。這項工具配備易於閱讀的儀表板，會使用者名稱及異常活動來顯示有風險的員工，QRadar關聯的發生事件。IBM Resilient 平台則是一套備受肯定的SOAR工具，可協助企業以自動化、流程標準化，以及運用合適安全工具回應各種突發資安事件。這項工具最大特色，在於能在不依賴人力的情況下，收集作業資料、提高生產力，縮短各種工作流程，加快威脅調查的速度。

「根據統計，隱藏於公司網路中的惡意程式，平均躲藏時間長達191天，且多半是由外部單位告知才發現。因此，一套先進安全分析解決方案有助於察覺最隱密的威脅，能在爆發資料外洩事件之前，即進行阻止。」IBM全球資訊安全部門全球威脅防禦產品協理謝明君說：「IBM QRadar Security Intelligence Platform 可為安全團隊提供精確偵測、設定優先順序、調查和回應等功能，提供分析威脅所需的能見度和分析功能。」

台灣數位安全聯盟理事長蔡一郎認為，企業應該從資源跟管理兩大面向建立合適的資安防護機制。

運用災情發大財 駭客攻擊力道增強

誠如前述，當全球陷入被COVID-19 疫情感染的恐怖中，駭客組織並沒有停止發動攻擊，反而趁此波疫情擴大攻擊力道，以便獲取更大的經濟利益。根據統計，駭客組織利用 COVID-19 危機的8大攻擊手法，分別為網路釣魚電子郵件、惡意APP、惡意網域、不安全的端點和終點使用者、供應商和第三方安全弱點、社交通訊APP和居家辦公、鎖定健康照護組織和熱點、利用未來疫後副作用和復甦中的弱點發動攻擊。

目前在暗網市場中，有駭客組織正在兜售以 COVID-19 為題的網路釣魚工具，有偽裝成新冠病毒爆發分佈圖的惡意郵件，價格從200到700美元不等。而常見的電子郵件主題，包特定行業的分析師報告、政府提供口罩，或其他有關營運和物流資訊的供應商，提供官方健康建議的詳細資料等。而根據調查發現，此類運用網路釣魚工具製作的電子郵件中，包含勒索軟體、鍵盤記錄程式、遠端存取木馬、資訊竊取惡意軟體等。

台灣數位安全聯盟理事長蔡一郎認為，企業應該從兩大面向建立

IBM全球資訊安全部門全球威脅防禦產品協理謝明君說，惡意程式平均躲藏時間長達191天，因此一套先進安全分析解決方案將能在爆發資料外洩事件之前即進行阻止。

合適的資安防護機制，其中以「資源」的角度著眼，無論設備、網路、系統、實體環境、存取控制等，應該強調在系統架構或平台的安全要求；至於「管理」的角度部分，則是人員、政策、管理制度等項目，應該強調在制度面建立與企業的需求。我們建議企業應該從針對資訊的取得進行限制著手，這部分可透過系統資源或是管理制度實現。另外，也應該強調縱深防禦，這部分則需仰賴網路架構與防護、系統平台安全、應用軟體安全等相互搭配才能達成。

「相較於國外仍然在疫情中掙扎，台灣仍然必須要注意以COVID-19 為名的可疑攻擊。」OWASP台灣分會研發長胡辰澔說：「駭客不會放棄任何可能的攻擊機會，所以企業在引進創新科技建構遠距辦公、在家辦公機制時，還是得將資訊安全放在首位。」

掌握數字背後意義 建置合宜防護機制

許多研究機構、資安公司，每年都會定時公布資安報告，藉此提供給企業作為資安防護機制的參考，然多數資安長都不了解背後的含義。以2020年九大網路安全統計排名，便包含「94%惡意軟體透過電子郵件傳送」、「在被報導的資安事件中，超過80%的成因來自釣魚攻擊」、「釣魚攻擊每分鐘造成17,700美元的損失」、「60%的外洩事件所利用的漏洞已經有修補程式，但卻沒有套用所致」、「63%的企業認為他們的資料在近12個月內可能因為硬體或晶片的漏洞遭到感染」、「針對物聯網設備的攻擊在2019上半年增加了兩倍」、「無檔案攻擊在2019上半年成長256%」、「資料外洩平均耗費企業392萬美元」、「有40%的IT主管認為網路安全的工作最難補足人力」。

戴夫寇爾股份有限公司執行長翁浩正指出，許多研究機構、資安公司，每年都會定時公布資安報告，然而多數資安長不一定了解背後的含義。

OWASP台灣分會研發長胡辰澔說，駭客不會放棄任何可能的攻擊機會，所以企業在引進創新科技建構遠距辦公/在家辦公機制時，得將資訊安全放在首位。

戴夫寇爾股份有限公司執行長翁浩正指出，仔細研讀前述9大與數字相關的資安訊息，前四項屬於攻擊手法、中間四項屬於漏洞管理，最後兩項則聚焦在損失與人。多數企業看到前述資訊之後，心中浮起的第一件事，恐怕都是「是否要購買新的資訊設備」，不過這種想法是錯誤的。

舉例而言，94%惡意軟體透過電子郵件傳送的訊息背後，代表電子郵件只是駭客入侵企業的媒介之一，最後目的在於竊取商業機密或消費者個資，若能建立妥善資料保護機制，就不需要擔心此數據持續攀升。因此，翁浩正建議企業應該要從全局視野觀看數據背後的意義，才能掌握背後的意義與關聯。