資安事件暴增 資訊長責任重大

CIO資安學院第1堂課

根據調查結果顯示，企業遭受資安攻擊平均付出成本高達 386 萬美元，且平均需要 69 天才能獲得控制。但若能在 30 天內快速回應並控制破壞行為，可以節省高達 100 萬美元以上的損失。

文／林裕洋

在獲取龐大經濟利益下，全球企業正遭遇日益嚴峻的網路安全威脅，根據趨勢科技公布的2019年資安預測報告指出，在人工智慧技術日益成熟下，駭客組織已開始利用該技術發動目標式攻擊，並且預測企業管理階層和特定對象的相關動向，進而取信周圍相關人士信任，以達到入侵企業網路的目標。然而同時間也有許多資安廠商，積極運用人工智慧模擬以偵測任何潛在的網路威脅，提供企業與消費者多層式的防護，抵抗來自四面八方的駭客攻擊。

在2019年第二屆CIO資安學院第一堂課上，關注資安趨勢多年的CIO協進會理事長盛敏成指出，企業要防範無所不在的資安威脅，應該要從認知、管理、技術三大面向著手，才能有效降低駭客攻擊帶來的衝擊，進而保護價值不斐的數位資產安全，為員工創造可專注於工作上的數位環境，實踐提升企業競爭力的終極目標。

建立事件回應制度 可降低營運損失

在駭客攻擊手法日益精進下，全球資安威脅呈現逐年上漲趨勢，也對企業造成極大的傷害。根據Ponemon Institute調查結果顯示，企業遭受資安攻擊平均付出成本高達386萬美元，且平均需要69天才能獲得控制。但若能在30天內快速回應並控制破壞行為，可以節省高達100萬美元以上的損失，顯見建立一套適當事件回應計畫，將有助於降低資安威脅帶來的衝擊。

然而現今多數企業都專注在強化安全措施，期盼達成對抗網路釣魚攻擊與勒索軟體，以及企業每天都可能遇到的所有其它大量的威脅。只是在攻擊手法日新月異的趨勢下，有全面防杜資安事件發生的難度很高，不如建立一套可執行的資安事件回應策略，才能有效降低駭客入入侵造成的損失。

台灣數位安全聯盟理事長蔡一郎指出，一套完善的事件回應制度，能協助組織回應突如其來的資料危害、或網路攻擊，目標是縮限潛在的危害，並確保公司可迅速恢復正常營運。

台灣數位安全聯盟理事長蔡一郎指出，一套完善的事件回應制度，能協助組織回應突如其來的資料危害、或網路攻擊，目標是縮限潛在的危害，並確保公司可迅速恢復正常營運。一套完善的事件回應計畫，分配清楚的職責、定義風險容忍度、事件分類、訂定明確的指示、優先移除與復原、從每個事件中學習教訓等，才能為企業打造穩固的營運基礎。

攻擊手法進步 不可僅靠資安設備

一套完善事件回應制度的首要工作，自然是先找出監督事件回應計畫的負責人，同時制定安全事件回應小組（security incident response team，SIRT），該小組將負責偵測、分類、通知、分析、阻遏、移除、記錄及事件後續活動。如此一來，才能在事件發生當下立即通知所有相關的利害關係人，並且收集各部門意見與分配職責，主動協調來自四面八方的意見。

面臨隨時可能發生的資安威脅，傳統做法都是一直在尋找最佳的解決方案，但是多數企業都忽略針對發生資安事件時的承受程度進行評估。在預算有限的狀況下，唯有事先決定資源優先順序，才能減少業務持續營運計畫與現況的落差，並找出公司營運所需的關鍵功能，並將資源優先放在做重要的事件上。

「每個事件都有可供學習的機會。一旦處理完事件，確認根本原因、分析、記錄、衡量並再度測試。評估用到的事件回應程序，以及它是如何進行的。」蔡一郎認為：「若能適時使用事件分析，尋找企業的偵測、通知程序、阻遏、移除或流程的缺陷或缺失，將有助於運用該資訊來加強事件回應計

畫，進而達成持續改善的事件回應制度，逐日大幅提升企業營運安全的終極目標。」

內部威脅增加 企業不可忽視

多數企業資安防護重點著眼於外部攻擊，然而根據CA report指出，有超過50%企業組織，在過去十二個月遭受以內部威脅為基礎的攻擊，90%企業組織明顯感受到內部威脅攻擊，且有25%受訪者表示比過去一年遭受攻擊頻率比過去更加頻繁。根據Ponemon指出，企業遭受惡意內部攻擊平均付出的成本為60萬美金，所謂內部威脅可能是員工無意間洩露資訊，配合外部實際利用竊得憑證的駭客組織，但也有可能是想要獲得好處或金錢的惡意員工。

根據統計，讓內部攻擊得以成功的常見失誤與問題，源自於過度的存取權限、存取機敏資料的裝置與位置不斷成長、觸及網路資料協力廠商數量的增加、利用USB這類外部儲存裝置、Dropbox等非IT核准app的缺乏控制。

戴夫寇爾股份有限公司執行長翁浩正認為，資安調查報告中，可發現受訪者公司回報的平均資安事件數量持續下降，從2017年148件減少到107件，關鍵在於企業開始重視駭客攻擊事件。

OWASP台灣分會研發長胡辰澔指出，雖然找出企業內部威脅很難，但若能注意被忽略的警訊，可在事件發生與資料離開網路邊界前，為企業組織提供潛在威脅事件的警告，如企業組織重大變遷、性格與行為的改變、員工離職、內部人員存取大量資料、未授權內部人員試圖存取伺服器與資料、授權但異常的內部人員存取伺服器與資料、試圖移出資料等。

試圖移出資料是指，大量下載資料至USB等外接裝置、大量上傳至Dropbox這種個人雲端app，或將大量大型附加檔案電子郵件寄到公司外部等工作。根據Cisco雲端資料外洩研究發現，有62%可疑下載發生在正常工作時間之外，有40%在周末執行。雖然數GB或TB的資料已屬於可疑活動的確切罪證，但要切記，機敏資訊也可以存在少量資料裡。

雖然沒有單一技術可能完全保護免於內部威脅，但結合資料外洩防護專案(DLP)、加密其他資料、靜止資料加密(encryption at rest)、身份識別與存取管理(IAM)、行為分析、特製事件記錄與事件管理，或許再加上蜂密罐檔案這類技術，可以降低資料被帶出網路之外的機會。另外，預防勝於治療，防止資料逃脫網路之外的最佳方式之一，即是針對企業組織裡可能有風險的員工，是建立一套完善的人員風險剖析機制，再搭配部門間合作、協調與溝通協助，自然是做好內部威脅管理專案的關鍵。

OWASP台灣分會研發長胡辰澔指出，雖然找出企業內部威脅很難，但若能注意被忽略的警訊，可在事件發生與資料離開網路邊界前，為企業組織提供潛在威脅事件的警告。

因應資安威脅暴增 全球資安預算增加

鑑於企業遭受資安攻擊的成本支出極高，根據知名資安顧問公司針對515名受訪者調查發現，因應2018年資安威脅風險升高，企業編列的資安預算也呈現同步成長的趨勢。根據調查顯示，企業平均資安預算。預算從1100萬增加到1500萬，成長幅度高達27%，這代表高階領導認定資安是企業最重要的徵兆之一。另有15%受訪者表示資安預算超過1000萬美元，但也有37%受訪者表示資安預算少於25萬美元，關鍵在於公司規模有極大差異所致。

此外，該份報告也指出資安長報告對象有所改變，25%受訪者指出資安長向資訊長報告，這比2017年調查結果上升了9%。另外，向董事會與科技長報告資安長人數，也分別從原本的6%、3%成長到8%、6%，而不論向誰報告，與董事會開會的比率也增高。38%受訪者表示每季與董事會進行資安會議，僅有19%受訪公司並沒有召開有關資安議題的董事會。

戴夫寇爾股份有限公司執行長翁浩正認為，資安調查報告中，可發現受訪者公司回報的平均資安事件數量持續下降，從2017年148件減少到107件，關鍵在於企業開始重視駭客攻擊事件。然而，大企業與中小企業有很大的落差，大企業回報196件，而小企業只回報了24件。不過光看回數量可能會失準，資安事件嚴重性其實有個更好的指標，在於組織是否必須通知某些個人或主管機關。

CIO協進會理事長盛敏成指出，企業要防範無所不在的資安威脅，應該要從認知、管理、技術三大面向著手，才能有效降低駭客攻擊帶來的衝擊，進而保護價值不斐的數位資產安全。

在資安公司進行的2018調查報告中，首次針對該問題進行調查，發現有24%大企業受訪者、12%中小企業受訪者表示，爆發資安事件時，必須通知受侵害事件影響的個人，另外有23%大企業受訪者、5%中小企業者必須向主管機關通報侵害事件。

DDoS流量創新高 仰賴專業夥伴協助

受惠於全球基礎網路日益健全，加上各類連網裝置持續問世，以至於問世多年的DDoS攻擊手法，對企業造成更嚴重的傷害，根據美國電信業者Verizon的最新DDoS趨勢報告，2018年上半年攻擊尖峰的規模，與去年同期相較出現了111%增長。2018年2月，軟體原始碼代管服務業者GitHub遭到每秒1.35TB攻擊，同年3月間，Netscout Arbor發現針對某家美國企業的每秒1.7TB攻擊，所幸這兩次攻擊都有業者提供緩解措施見效，網路服務並未中斷。前述事件顯示，傳統資安資安設備根本無力敵擋大規模DDoS攻擊，唯有仰賴專業資安公司協助才能降低營運風險。

盛敏成指出，由於駭客組織已能透過多元管道接觸越來越多電腦，並藉這些電腦發動DDoS攻擊，而多數人根本不知道物聯網設備，是否成為被駭客發動DDoS攻擊的目標。此外，在資訊交換速度加快的前提下，只要有人開發出新的攻擊手法，網路犯罪者馬上就會想辦法利用它，或將它納入僵屍網路工具包，也導致DDoS攻擊事件不段發生。

因應此DDoS攻擊規模日益擴大，企業不妨從8個方向著手，分別是準備好DDoS緩解計畫、能夠做出即時調整、獲得DDoS保護與緩解服務、別只靠週邊防護、對抗應用程式層級的攻擊、與同業合作、注意次要攻擊、保持警覺等，才能避免陷入DDoS威脅之中。 CIO