解決資訊不對稱是確保資訊安全的關鍵

現今企業花費愈來愈多的資安預算，卻也面臨空前嚴峻的網路安全挑戰，安全顧問公司戴夫寇爾則認為，解決資訊不對稱，才能確保企業網路的永續安全。

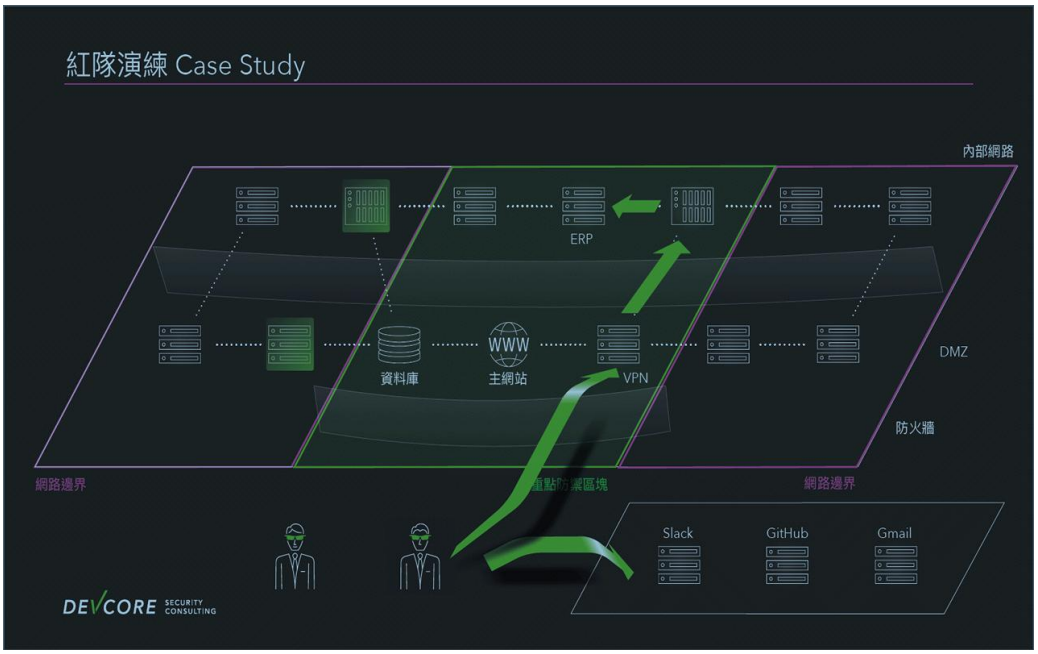
戴夫寇爾執行長翁浩正一語點破今天企業組織資安的問題，在於企業不是買的設備不夠多，而是防錯重點。就像一個國家大興土木建起高高的城牆，然而他們的敵人卻開起了飛機；如果不知道敵人的動機、資源或盤算，資安投資也可能枉費；反過來說，企業花了大筆經費強化網路防火牆，但卻忽略資安教育，致知資安意識薄弱的員工在公司下載盜版軟體或不小心點選到惡意連結造成感染。因此，企業和政府面臨危險來自資訊不對稱性。

(DEVCORE 執行長 翁浩正)

他指出，資訊不對稱性因攻擊方更大的攻擊規模、更低的技術門檻、更強運算能力及更刁鑽高明的攻擊手法而雪上加霜。今年三月全球最大開源程式碼社群網站 Github 遭遇 1.35Tbps 的分散式阻斷攻擊(Distributed Denial of Service, DDoS)，導致斷線 5 分鐘；3 天後網路安全設備商 Arbor Networks 遭到更大的 1.7Tbps DDoS 攻擊。所有企業包括電信業在內，面臨 TB 等級的超大攻擊幾乎無一招架得住，但未來這類攻擊可能會愈來愈頻繁。其次，攻擊的技術門檻愈來愈低，原因並非天才駭客更多，而是網路公開販售攻擊工具以及代客攻擊服務，駭客不需強大技術即可買到攻擊武器，甚至可以花錢請人發動攻擊，因此攻擊門檻愈來愈低。

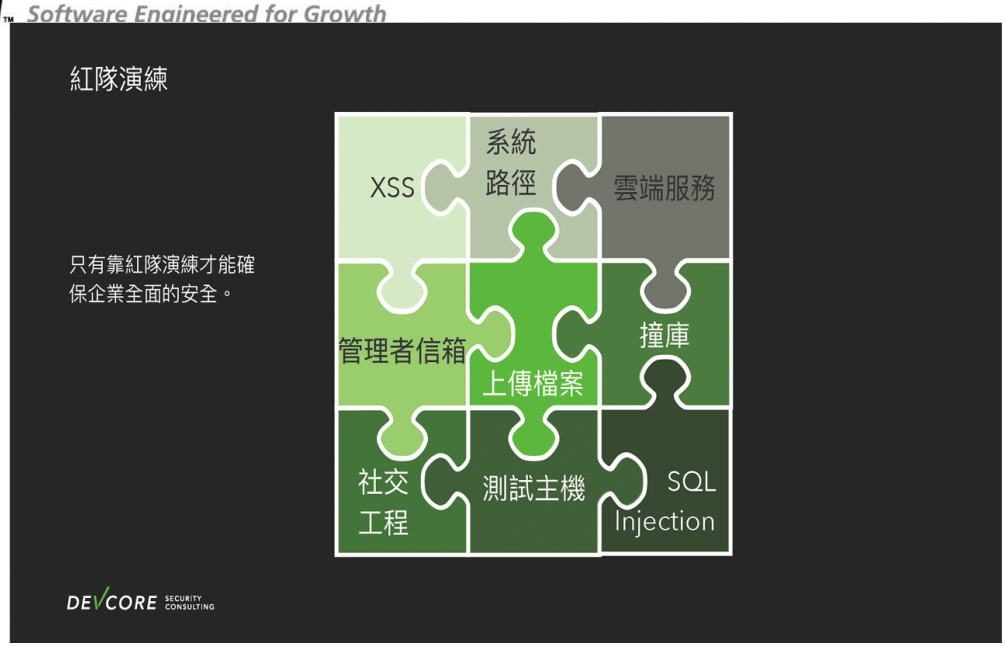
此外，更強大 GPU 加持的運算效能，使過去困難的密碼暴力破解也變得容易。以 MD5 演算法產生的 8 字元密碼為例，一名駭客若使用 8 張 nVidia 顯示卡組合的機器，破解常見的數字＋英文字母大小寫的密碼組合只要 18 分 12 秒，而由所有 ASCII 可視字元組成的密碼，也只要 9 小時多即可破解成功。對駭客來說是報酬率極高的投資。「暗網」為代表的網路黑市，讓駭客可以取得各種漏洞、攻擊工具，以及各種攻擊情資資料庫（如可被攻擊的 IP 位址、外洩的帳號密碼或信用卡資訊），使駭客可組合各種漏洞和情境，以更刁鑽的手法達成滲透主目標的任務。

上述種種新趨勢也讓傳統安全防禦方法效果降低，必須有更新的防禦思維。首先，企業必須認清他們的對手不是單一駭客，而是整個網路黑市產業。這個「產業」的商業模式出售各種「客戶」需要的目標資訊，像是銷售個資、郵箱、信用卡號給詐騙集團、販賣帳密、個資資料庫、攻擊程式及情資給駭客組織。另一點很重要的是，駭客並不會攻擊企業部署防護最嚴密的地方，例如駭客不會浪費時間來強攻網路銀行，而是入侵網銀系統的測試網站，因為這裏往往疏於防護，之後再橫向移動入侵網路邊界。和戰場上一樣，資安防禦也要充份了解自己的弱點及敵軍的目的、動機，站在詐騙集團、駭客組織的角度來構想防禦策略，才能化解資訊不對稱的情勢。



（駭客往往會透過邊界防禦較為薄弱的管道，先入侵到企業內部系統後，再透過橫向移動的方式，竊取鎖定的重要資料）

這就是紅隊演練(Red Team Assessment)的價值所在。和過去企業常採用的弱點掃瞄等自動化工具相比，以人類執行的紅隊演練更能模擬出駭客如何將漏洞組合利用。它又和滲透測試服務不同，紅隊演練不是著眼於漏洞，而是在不損及企業利益前提下，在有限時間內無所不用其極的方式入侵、攻擊各種可能的進入點，以達成企業指定的測試任務（如取得客戶資料）。它是從攻擊者角度來尋找所有可能的入侵途徑。簡單來說，它能彌補滲透測試的不足。



（紅隊演練可以找到從各種管道而來的攻擊）

在這樣攻擊等於營利的時代，戰場遠比企業想像得更大範圍，更難防禦，戰略思維比購買武器更重要，對擁有豐富機敏資訊的企業及政府單位來說，紅隊演練可協助盤點弱點、化解資訊不對稱，達到「知己知彼、百戰不克」的目標。