處於物聯網世代，網絡攻擊種類繁多，中信國際電訊CPC早已洞悉先機，為企業提供一系列託管式安全解決方案。

中信國際電訊CPC信息科技及安全服務部
顧問及服務交付經理
林慕歡

2016 中小企最佳營商夥伴 THE BEST SME PARTNERS
Economic Digest 經濟一週

中信國際電訊CPC

技術為先 全面信息安全管理

科技及互聯網發展一日千里，雖然為人類帶來不少的便利，亦為企業帶來無限商機，但同時卻吸引了世界各地的駭客進行攻擊，以圖謀利或威脅企業的數據安全。為了防禦層出不窮的網絡攻擊，企業必須透過合適的信息安全解決方案，全面管理及監察其網絡及數據安全，以免構成商譽和金錢損失。中信國際電訊CPC一直對各種科技趨勢非常關注，因此往往早著先機；例如早於2006年，便已經深諳信息安全的重要性，致力提供多元化及一站式的信息安全管理服務。時至今天，中信國際電訊CPC已成為行業領先者，為最新的安全威脅提供解決方案，備受行業及客戶認同。

駭客的攻擊手法變化多端，而且愈見精密及具針對性，然而不少的企業，尤其是中小企，由於缺乏信息安全知識及專業的技術人員，往往對網絡及數據疏於管理，因而時刻都備受安全威脅。

中信國際電訊CPC信息科技及安全服務部顧問及服務交付經理林慕歡指出：「駭客的攻擊技術不斷提升，3年前更開始盛行APT（進階持續性威脅），即駭客透過研究網絡使用者的習慣，從安全級別較低的渠道進行病毒滲透，如滲入電郵、流動應用裝置、網頁等，再進一步入侵使用者或企業的電腦系統，開始盜取機密資料，又或進行惡意刪除，甚至藉加密該等資料，對使用者或企業進行勒索，引致嚴重損失。」

「就如今年台灣某家銀行，便發生了提款機被植入惡意程式事件，共有41台ATM中毒，變成吐鈔機，遭盜取的金額高達8千餘萬台幣，損失嚴重。此外，全球已逐漸進入IoT物聯網（Internet of Things）世代，即所有日常生活、企業運作都趨向依賴網絡科技互聯互通，使入侵者有機可乘。因此懂得如何防禦惡意程式，及早修正問題，實在是企業不可忽略的重要一環。」

全天候監察 實時修正漏洞

中信國際電訊CPC推出的TrustCSI™——系列託管式安全解決方案，服務範圍包括全面的預防、偵測、修正、持續監察客戶的系統等等。此方案有助企業免卻投放大量資源，便可擁有符合他們特定安全需要的解決方案。

TrustCSI™系列以ISO27001信息安全管理認證程序為基礎，由擁有安全認證的專家團隊管理，而中信國際電訊CPC安全運作中心（SOCs）配置了先進的安全信息及事件管理（SIEM）技術，可作24x7全天候的監察，每天追蹤數以十億計事件，將數據與資料庫作分析，假若發現事件關聯結果高於用戶設定的水平，將會啟動事件反應機制，並為企業提供實時的警報，讓企業可在受到網絡攻擊前，採取即時的矯正行動。

在云云的TrustCSI™解決方案中，TrustCSI™ ATP進階威脅防護服務便可謂解決惡意程式及勒索軟件的最佳方案。它整合了能為企業網絡作多層保護的「統一威脅管理（UTM）」、抵擋進階網絡應用威脅的「網絡應用防火牆（WAF）」、抵禦各種電郵安全威脅的「電子郵件安全設備（SEG）」及能過濾附有病毒檔案的「沙盒（Sandbox）」等4大完善配套。

透過上述4大組件，TrustCSI™ ATP能無縫監察檔案、電郵、網絡流量及網絡應用各大層面的可疑活動，全面地支援企業對抗進階網絡威脅及攻擊。此外，更配合了TrustCSI™ MSS安全管理服務，為企業預防、偵測及修正信息安全基建及系統上的漏洞，達至協同效益，讓企業全面抵禦對端點、網絡及伺服器的進階持續性威脅。

投放資源 致力培育人才

中信國際電訊CPC的專業團隊，擁有豐富經驗及專業知識，能迅速回應網絡攻擊：「公司非常重視人才，因此投放大量資源於培育人才。團隊各人都需要接受嚴格的第三方認證培訓，以及持續的在職及實戰訓練。而當完成處理一些特別的安全事件後，我們都會作出事後分享及檢討，從而不斷提升服務及技術水平。」

林慕歡又指：「未來我們將會更善用大數據（big data）及加強推廣TrustCSI™ MSS的應用，再加入機器學習技術（machine learning technology），以數據分析企業系統上的異常行為（abnormal behavior），從後推斷前因，使更有效助客戶及早預防網絡攻擊。」