IT Square 編輯之選2016 總選特刊

EDITORS' CHOICES 編輯之選 IT Square

中信國際電訊CPC再奪「最佳資訊科技綜合服務夥伴大獎」

創新方案 擴展基建 全面滿足企業ICT需求

中信國際電訊CPC一直創新不斷，致力提供一系列嶄新ICT方案，配合企業不同的發展需要。其中雲運算、信息安全，雲數據中心及網絡服務更是當中四大旗艦產品，為客戶提供一站式服務，抓緊每個機遇。

■中信國際電訊CPC銷售部總經理范俊倫（左）及信息科技及安全服務部高級副總裁鄺偉基（右）。

去年，國際間發生多宗入侵網絡事故，保安事故不絕如縷，部分因為入侵手法高超，防不勝防；另外則是IT迅速轉型，保安技術未能追上形勢所致。

更嚴峻的是，全球皆嚴重缺乏網絡保安專才，難以延聘人手。面對嚴格監管和法規，加上流動技術、雲運算、辦公室器材智能化、IoT普及；保護資訊難度更高，外判IT保安服務，蔚然成風。

市場上不少信息安全管理服務（Managed Security Services），透過全天候「安全運作中心」（Security Operation Centre，SOC），提供監察和分析服務，如防火牆和入侵防禦系統（Intrusion Prevention System）管理，甚至通過先進的安全訊息及事件管理（SIEM）技術，從網絡設備蒐集的日誌檔（logfile）中作關聯分析，找出真正威脅事故，阻截攻擊。

但是，信息安全管理服務還須配合適當技術，才能追上形勢，迎接新一代IT保安挑戰。

中信國際電訊CPC的TrustCSI™信息安全管理方案，全面預防、偵測及修正網絡威脅；再配合中信國際電訊CPC安全運作中心24x7全天候監察，實時發出安全事故警報。

保安技術不斷演進

多年來，中信國際電訊CPC與多家國際著名保安設備供應商合作，不斷引入創新技術和推出新的方案，全面保護企業的網絡安全。

中信國際電訊CPC信息科技及安全服務部高級副總裁鄺偉基說，隨著入侵手法演進，IT保安也不能不求變，必須發展新一代保安技術。

不少企業受進階持續性滲透攻擊(APT)的威脅，並造成嚴重損失，當中包括不少金融界機構。去年，金管局發出通知，要求金融機構正視APT；中信國際電訊CPC引入著名保安設備供應商的最新技術，推出針對此新興威脅的TrustCSI™ ATP進階威脅防護服務，方案整合了統一威脅管理（UTM）、網絡應用防火牆（WAF）、電子郵件安全設備（SEG）、沙盒(Sandbox)及全天候的信息安全管理服務（MSS），有效堵截APT入侵。

「首先，TrustCSI™ ATP解決方案有助客戶速致法規遵從需要，符合本港甚至海外監管當局要求。TrustCSI™也能協助客戶，符合本港以至新加坡上市和金融規管。」鄺偉基說，但即使金融機構完全遵守法規，防禦也絕不能因此鬆懈。

機器學習準確辨識未知威脅

鄺偉基說：「例如，不少資訊保安總監（CSO）逐漸認識到『零日攻擊』是IT保安最大隱憂。惡意軟件可輕易變種，避開偵察軟件，部分惡意軟件更屬於度身訂造，導致傳統防禦失效。IT保安業界早有共識，單憑惡意程式的「特徵偵測」（Signature-based Detection），例如檢查檔案獨有的Hash值，以過濾和偵察病毒，已無法有效杜絕惡意程式。故此，保安技術引入機器學習和數學分析，以無特徵偵測（Signature-less detection）未知威脅，包括APT，是必然趨勢。」

中信國際電訊CPC擁有業內最有經驗的信息安全專家團隊，分析大量日誌檔的關聯數據，即時偵察保安異常行為。隨著網絡設備大量湧現，加上惡意程式更難於被發現，因此有必要引入新技術，以確保客戶受更周全保障。

TrustCSI™所採用的新技術，即使沒有指紋檔（Signature）亦可發現未知威脅，原理是運用數學模式；採用統計學的Bayesian Probability Theory，或稱為有條件的統計或然率計算，收集相關聯的數據去建立一個基於客戶環境的獨特行為模型；再與即時數據進行差距分析，以預測另一項事件出現的可能性以及異常的可能性。

「一部主機若受了感染，如果只集中分析主機本身日誌檔，可能找不到任何蛛絲馬跡。」鄺偉基說：「因為先進病毒懂得自我隱藏，甚至修改日誌檔，刪除相關記錄；也可暫時按兵不動，避過掃描的各種關卡。」

但病毒要在系統內盜竊或破壞，必須有所行動，過程中產生異於平常的行為，此時網絡上的數據與已經建立的行為模型將有所差異，因此能通過進一步的數學分析以推斷發生安全事件的可能性。再深入一步，將其他主機的不尋常連接，或登入方式和時間等等相關現象再進一步對比，預示另一些設備被感染的可能性。

TrustCSI™的新偵察技術，甚至馬上錄下可疑數據，可以『重播』（Playback）重新呈現連接紀錄，病毒入侵和感染的整個過程。鄺偉基表示數據包截獲（Packet capture）的數據可供保安專家進一步深層分析和搜證，甚至作鑑證（Forensics）之用，掀出受攻擊的源頭。

鄺偉基續說：「曾經有企業客戶在進行文件批核過程中，未經負責人過目，竟自動被審批，起初以為發生入侵，後來利用TrustCSI™的新偵察技術，發現原來編寫流程出錯，文件無意之間遭自動批核。鑑證功能可破解設計過程中安全漏洞，縮短除錯過程。」

迎接IoT時代保安

鄺偉基表示，新技術的另一優點，足以應付極之龐複網絡環境，迎接未來IoT時代挑戰。

流動和IoT設備迅速增長，加上雲運算和網絡應用的普及，IT防線更長。接入設備愈多，也更難堵塞所有漏洞弱點；有些設備，甚至廠商停止了支援，無從獲取修補軟件。

「去年，台灣某銀行的提款機，遭受黑客入侵；然後操控提款機（ATM）自動吐出7000萬新台幣，引起了金融界的嘩然。」事後，台灣執法機構迅速公佈病毒Hash數值，同業可快速偵察，避免了病毒漫延。是次病毒感染提款機事件，令金融機構馬上意識到，有些設備難以監察保護，所謂『漏洞管理』（Vulnerability Management），根本上不可能周全。」

提款機可算屬於智能周邊設備，作業系統卻不經常更新，更可能成為弱點。近年，網絡威脅已不限於主機或桌面電腦；病毒黑客轉攻流動設備，甚至是IP監察鏡頭、網絡打印機、視像會議，甚至連感應器和溫度控，都成為了攻擊目標，企業也更重視網絡登入控制（Network Access Control），從接入點加強防禦，也無從達到百分百保護；仍有機會掛一漏萬，病毒從其他弱點乘虛而入。

TrustCSI™信息安全管理服務所提供的大數據分析和機器學習能力，能針對上述新形勢，實時監察現場所有網絡活動，一旦發現異常就錄下該段活動封包，SOC再深入分析，即時判斷是否受到入侵。

事實上，機器學習更加完善了信息安全的監控，單純利用SIEM分析的方案缺乏了結合即時客戶自身行為的獨特性。如果未能將所有日誌檔加入分析，或者黑客控制了主機，而修改了日誌檔，都會導致SIEM無從發揮該有的作用。新技術的加入就能通過統計，從周邊活動和機器學習，計算出某部設備不尋常活動，從而推斷發生安全事件的可能性，SOC則同步對相關事件進行深入的分析。

DataHOUSE™雲數據中心 助企業拓展全球業務

除了針對未知威脅的保安，隨著數碼化轉型，IT基建亦已成為現代企業拓展業務的先頭部隊：ICT服務供應商可提供跨國的網絡連接、數據中心、雲運算等服務，助企業快速拓展海外業務。

另一方面，經營不斷全球化，企業也須遵從各地的法規：從數據安全、環境管理、數據所在地（Data Residency）和數據主權（Data Sovereignty）等，皆面對更加嚴格的規管。不過，服務供應商亦正致力協助客戶克服挑戰。

中信國際電訊CPC所經營業務，全部均針對跨國企業需求而設，提供標準化和一站式服務，支援跨國業務；其中包括了TrueCONNECT™ MPLS VPN服務、SmartCLOUD™雲運算服務、TrustCSI™信息安全管理，以及DataHOUSE™企業級雲數據中心四大業務，涵蓋了虛擬專用網絡連接、雲運算、資訊保安及數據中心的整全ICT方案。

目前，DataHOUSE™全球設有29個雲數據中心，並取得國際管理標準ISO認證。而各項IT基建之中，數據中心所佔成本相當高；原因之一是管理和維護數據中心；從供電、後備電源、空調冷卻、防火保安、連接監控等各項設備，必須極其可靠，甚至遵從法規要求。另外，數據中心維護成本更不輕，外判數據中心服務，企業可專注於業務發展，不單可減經成本，也較易符合各地法規要求。

現時，不少地區開始關注環保和節能，每天數據中心消耗大量能源，須符合節能減排等目標。不少地區的條例，陸續加入企業可持續發展和環境責任條文，甚至納入了上市要求。

數據中心回應環境訴求

兩年前，香港交易所亦發表文件，闡述了全球交易所，不約而同採取推動企業社會責任（CSR）措施，包括提高上市公司在環境、社會、管治（Environmental, Social and Governance，ESG）等的意識和承擔，推動企業公佈CSR／可持續發展等報告。今年一月，本港上市公司亦須按規定公佈有關資料，否則須解釋理由；其他地區交易所亦紛紛有同樣要求。上市公司公佈ESG，確保企業達到了客戶和投資者，對該企業承擔社會責任的期望。

中信國際電訊CPC銷售部總經理范俊倫說，DataHOUSE™早已積極改善各地雲數據中心的節能和減少碳排放，幫助上市公司分擔社會責任，並符合CSR／可持續發展等報告的ESG公佈要求。

DataHOUSE™服務取得多項ISO認證；包括了ISO 14001環境管理體系認證；也就是須確保企業發展業務同時，也不忽略保護環境。ISO 14001認證代表企業的數據中心，已符合ESG環境責任的部分要求。

保安認證全面保障

數據中心另一重要要求為資訊保安，而DataHOUSE™亦很早已取得ISO 27001信息安全管理體系認證。除了國際認證和安全標準，DataHOUSE™最近也通過了新加坡金融管理局「威脅及弱點風險評估」（Threat and Vulnerability Risk Assessment；TVRA）規管要求。

鄺偉基說：「數據中心安全措施；包括了連接、管理、存取、人員出入的各項程序規定，DataHOUSE™雲數據中心達致的安全水平，比不少自行籌建的數據中心更高。」

不少數據中心用於與地容災（Disaster Recovery）和數據備份，以求達致商業持續的規管要求。中信國際電訊CPC在全球有超過100個網絡據點（POPs），DataHOUSE™均以TrueCONNECT™虛擬專用網絡互連，具有高度可靠性和抗災能力，供不少客戶容災和備份之用。

范俊倫說：「DataHOUSE™是少數符合多項國際認證的數據中心，在內地主要城市亦有據點，不少國際企業打入中國市場，均借助DataHOUSE™加快進程，快速部署位於各地業務。DataHOUSE™符合上述國際標準和監管機構要求，毋論部署於任可地點，均保持一致水平。」

中信國際電訊CPC不斷擴大DataHOUSE™覆蓋和數量，除現有的29個數據中心外，今年將於北京和廣州新增兩座數據中心，全球數目將增加到31個。

助力開拓一帶一路商機

范俊倫說，中信國際電訊CPC二月初剛完成收購歐洲電訊商 Linx Telecommunications旗下的電訊業務，業務範圍延伸至中亞及中、東歐市場，覆蓋了中國「一帶一路」經濟帶的沿線地區。是實上，是次項目包括多個增長潛力優厚的市場；從俄羅斯、東歐、中亞，以至卡薩克斯坦和多個「斯坦」區域。

「愈來愈多中國內地和香港公司，以港澳作為跳板和橋樑，發展歐洲和中亞市場。Linx Telecommunications具備了基建優勢，包括一條長達470公里，橫跨波羅的海海底光纖網絡，可交付最低延遲、最高速廣域連接至歐洲和中亞。另外，Linx Telecommunications人員熟悉當地文化、語言、監管環境；而位於塔林的數據中心更是愛沙尼亞最大的互聯網交換中心（TLL-IX），相信這次收購不但可帶來更多商機，更有助提升公司的整體營運效率，為未來發展更上一層樓。」

范俊倫說，中信國際電訊CPC的網絡服務已覆蓋中國、東南亞、中亞、歐洲等地區，為客戶提供端對端的一站式服務；再配合DataHOUSE™雲數據中心服務，客戶可快速部署連接和運算能力，毋須與多家電訊商和服務供應商協調，大大減輕工作負擔。

鄺偉基說，不少中亞國家充滿商機，Linx Telecommunications在歐亞有大量技術人才，嫻熟當地語言和合作伙伴，中信國際電訊CPC與Linx Telecommuncations正就服務交付程序作出最後整合，客戶若計劃在歐洲部署業務，所獲服務體驗，甚至服務承諾，均完全一致。

范俊倫最後補充說，企業無論於任何地區開展業務，數據中心和網絡服務幾乎是先決條件，而資訊安全及運算能力更是不可或決。中信國際電訊CPC的全面 ICT 服務正可配合所需，為客戶帶來最佳用戶體驗，有助找緊商機，早着先鞭。