網絡科技的發展緊隨時代發展的變化，現時雲端運算已成為不少商業企業的基礎設施，使企業能夠更快速地部署及運作應用程式，降低管理及維護成本，帶來無數實質性的利益。不斷演變的雲端運算技術卻同時帶來資訊及數據安全的問題，現時最大的挑戰就是APT進階持續性滲透攻擊（Advanced Persistent Threats, APT），一種隱形而對企業具殺傷力的威脅。

11月中，中信國際電訊CPC聯同Imperva及Palo Alto Networks舉辦名為「破解APT之謎：拆解APT攻擊的最有效方法」論壇，邀請業界專業人士和與會者分享如何減輕APT的潛在風險的經驗與心得。論壇由羅兵咸永道會計師事務所合夥人黃景深主持，並邀得品誠梅森律師事務所合夥人Paul Haswell作嘉賓，聯同主辦單位的講者，包括中信國際電訊CPC信息科技及安全服務部高級副總裁鄺偉基、Imperva亞太及日本區安全系統總監Vladimir Yordanov，以及Palo Alto Networks香港及澳門區總經理王衍恒和香港及澳門區系統工程經理耿強，一起就議題分享心得。

無所不在的APT威脅

APT攻擊比以往任何網絡安全威脅更加複雜，鄺偉基表示，2013及2014年，企業面對APT攻擊較以往增加不少，網絡安全面對的威脅愈來愈複雜、持續、隱蔽，給企業帶來莫大隱憂。黑客可以用企業網絡中的任何安全漏洞，危害整個數據庫。Paul Haswell道：「數據是企業最重要的元素，由此衍生了數據交易市場。」若企業數據安全出現漏洞，被黑客惡意竊取，「被攻破的數據庫將為企業帶來難以估計的損害，已非單純誰要負責的問題。」

以往黑客發動的APT攻擊以政府為主要目標，近幾年黑客攻擊的性質發生了變化，使一眾企業人心惶惶，傳統的網絡安全系統更加形同失效。受薪黑客隱身進行具針對性和具體的APT攻擊，使企業更加難以檢測和阻止。隨着科技的進步，移動設備、雲端系統，甚至高科技家電均可能成為安全缺口，使黑客輕易入侵數據庫。


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強調培育企業人才有效使用雲端運算系統是最重要的。


Imperva亞太及日本區安全系統總監Vladimir Yordanov認為企業必須加強警覺性，未雨綢繆，才能及早避免惡意黑客的APT攻擊。

減輕APT的風險

要減輕APT的風險，我們需要擁有比傳統防護系統更先進的做法，除了新科技外，教育人們安全理念及做法也同樣重要。鄺偉基說：「人們意識到網絡安全的重要，但他們往往不知道該怎樣做。」不少企業投入大量資金打造最先進的網絡安全環境，但更重要的是要有效地使用這些設備。「我們要教育客戶，技術無疑非常重要，但釐定安全工作流程以及掌握妥善處理安全事件的技巧更加不容忽視。」中信國際電訊CPC建議企業的安全專家需擁有國際認可專業資格，並熟知安全工作流程，才能有效保護企業避免APT攻擊。企業亦可考慮選用可靠的第三方供應商的服務，透過其富有實戰經驗的專家團隊及先進技術，保障企業安全。

「企業必須解決的另一個關鍵問題是偵測和預防之間存在的差距。」Vladimir Yordanov說。企業往往過於集中檢測病毒和惡意軟件，卻忽略解除潛在威脅所需的舉措，導致未來可能需要做出更多補救措施。鑑於保障網絡安全的艱巨及複雜性，很多企業都選擇將安全解決方案外判。Vladimir Yordanov指出，將安全解決方案外判並不意味着企業本身便毫無責任。王衍恒續分享道，企業需要有自身數據的決定權，不應將敏感的數據庫全交由外判商打理，更需慎選可靠的服務伙伴與清楚哪些信息是可以安全外判，而哪些只能夠內部處理，才能保障企業數據庫可靠，減少受到攻擊的可能。

五位嘉賓在論壇講解APT的特徵和對抗APT的方法

新時代的集體解決方案

這次論壇將中信國際電訊CPC、Palo Alto Networks和Imperva聚在一起，為企業提供有效和全面的安全解決方案服務，以拆解潛在的APT威脅，保護企業數據。

以Palo Alto Networks為例，他致力於為應用程式提供前所未有的可視性和分級控管功能，啟動最新端點至端點（end to end）安全應用程式。耿強認為新一代的安全平台必須具有三個重要元素，第一是新一代防火牆允許安全訪問應用程式，第二是智能雲端網絡系統可自動偵測並消除安全威脅，第三是能確保端點安全，檢測及識別任何來自端點的潛在威脅。

Imperva亦開發了先進的安全系統，例如Vladimir Yordanov所介紹的Skyfence，便是一個專為雲端應用程式提供可靠及安全服務的平台，可以識別任何連接到用戶網絡的雲端應用程式，跟蹤訪客，檢測網絡異常動態。

先進科技固然重要，但專業服務亦不可少。中信國際電訊CPC除了與上述兩位合作伙伴合作，提供相關的安全技術外，更以安全信息與事件管理（SIEM）技術提供『安全服務』，透過其安全運作中心將在不同安全設備收集回來的數據與資料庫作分析，並將結果分類及找出安全風險機會率。『專業服務』方面，中信國際電訊CPC擁有獲得安全認證的專家團隊，並配以信息評估服務為客戶作漏洞管理，以消除更多安全威脅。鄺偉基指出：「將『安全服務』結合『專業服務』，創建一個新的理念，為客戶帶來『信心服務』，正是中信國際電訊CPC的服務方向。」

總括來說，安全不是單一供應商要負責的解決方案，而是整個行業及企業本身都應該負的責任，只要一起努力，安全威脅定能迎刃而解。

（數據及資料由中信國際電訊CPC提供）


Palo Alto Networks香港及澳門區總經理王衍恒建議企業若尋求安全解決方案外判商的幫助，亦應負起為公司機密資料把關的責任。


Palo Alto Networks香港及澳門區系統工程經理耿強和與會者分享安全應用程式如何有效協助企業消除安全威脅。