預防企業級網絡攻擊

中信國際電訊CPC 整全方案應對APT威脅

近年進階持續性滲透攻擊(Advanced Persistent Threat，APT)對企業的影響日益明顯，然而由於企業對APT認知不足，往往疏於防範。要有效應對APT攻擊，絕不能單靠傳統防火牆等簡單防衛，而是要針對APT的攻擊形態，從「六大階段」對症下藥。中信國際電訊CPC的TrustCSI™是一系列的託管式安全解決方案，其中的TrustCSI™ MSS(安全管理服務)便配備先進的SIEM(安全信息及事件管理)技術，在該公司旗下的安全運作中心(SOC)運作，為企業提供24 x 7全天候監控服務；再加上其他TrustCSI™方案，例如MAS(網絡應用程式安全託管服務)、MFS(託管式防火牆服務)及IAS(信息評估服務)等，能針對六大階段，幫助客戶全面預防、偵測及修正APT威脅，令你毋須再為企業安全憂心。

▲鄺偉基認為應對最新的APT攻擊形態，應從「六大階段」對症下藥。

APT攻擊是利用先進的黑客技術，入侵並潛伏在一定數量的電腦中，到有需要時即發動攻擊，竊取客戶的重要資訊。它的特性是潛伏期長、隱蔽性高，因此往往令企業防不勝防，造成重大損失。

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認為，本港不少企業的防範意識非常不足。他指出：「據Hutchins & Cloppert在第六屆信息安全國際峰會(6th Annual International Conference on Information Warfare and Security)上的報告，APT攻擊可被分作六個階段。要有效阻截APT，就要從每個階段入手。」

六大階段 全方位偵測消除APT

APT攻擊的六個階段分別為：偵測(Reconnaissance)、武裝(Weaponization)、傳遞(Delivery)、啟動操作(Exploitation)、指揮控制(Command & Control)及竊取(Exfiltration)。黑客首先會物色防範薄弱的系統(偵測)，繼而將惡意程式寫入普通文件(武裝)，並傳送給目標企業(傳遞)。當企業人員打開文件時，程式便會植入電腦(啟動操作)，並控制該伺服器，以傳送更多惡意程式予其他電腦，製造更多殭屍電腦(指揮控制)。接着程式便會隱蔽，待時機成熟便一舉偷竊目標的資訊及財產(竊取)。

企業如果單靠傳統防火牆應對APT，往往未能防禦已經潛藏的APT威脅。鄺偉基補充道：「APT可以潛伏相當長的時間而不被發現，以DarkHotel為例，它早在二〇〇八年已經植入目標的伺服器。防火牆及防毒軟件對這些潛藏已久的程式，往往難以察覺，因此單靠防火牆並不可行。」

TrustCSI™服務 針對六大階段擊退APT

TrustCSI™一系列的託管式安全解決方案則兼顧預防、偵測及修正三大功能，可兼顧APT不同階段應對策略，助企業及早偵測、並消除隱藏病毒，幫助企業在上述的六大層面應對APT攻擊。

其中的TrustCSI™ MAS及TrustCSI™ MFS設有的主動安全事件管理及回應、實時監控、特定政策、攻擊報告等多樣功能，助企業阻截不同形式的APT攻擊。而TrustCSI™ IAS則針對潛伏的APT，它的特別設計可準確又快速地確認基建及網上應用漏洞，並同時提供矯正步驟建議以及阻絕威脅技術。此外，TrustCSI™更能提供沙箱環境(sandbox)以測試有可能包含病毒或其他惡意代碼的程序，避免該軟件危害企業主機裝置。

TrustCSI™ MSS 最強監控管理

上述的解決方案並由TrustCSI™ MSS作全面監控，在不同的安全裝置記錄下來的各種原始事件數據，會被傳送到中信國際電訊CPC的安全運作中心(SOC)進行分析。這個獲得ISO9001、ISO14001、ISO20000及ISO27001國際認證的世界級安全運作中心有專人作廿四小時監控，並配備先進的SIEM技術，能即時將數據分析及有效分類，計算企業的安全風險機會率。

一個優秀的監控管理服務，應該能為企業辨識真正的安全威脅。鄺偉基補充指：「網絡上每秒指令碼可達億計，而當中即使有惡意程式，也不一定會威脅企業。例如惡意程式的目標是Linux系統，但攻擊終端其實是微軟系統的話，其實便對客戶沒有威脅。我們的SIEM技術加上專業團隊，正可精確地識別真正威脅，而不須事事驚動客戶。」

企業只需明白APT攻擊的六個階段，慎選合適安全方案，便可防患未然，或對有關攻擊作即時制止及修正，將APT的威脅減至最低，確保公司財產得到妥善保護。

(資料由客戶提供)