中小企的最佳保鑣

中信國際電訊CPC TrustCSI™托管式安全解決方案

早前有本地航空公司發現其企業系統存在可疑活動，有大量客戶個人資料被洩漏，讓廣大客戶為之震驚。事實上資料外洩及黑客入侵方式不斷改變，技術也不斷提升，當連大企業也不能倖免，中小企更難以靠自己來抵禦，因此，中信國際電訊CPC的托管式安全解決方案便成為中小企的最佳保鑣。

中信國際電訊CPC資訊科技高級經理鄧志明表示，TrustCSI™ Secure AI方案以人工智能分析惡意軟件行為模式，來分辨可疑網絡活動，以防止黑客入侵。

面對黑客攻擊，最重要是反應快速。事實上從來沒有系統是完美、沒漏洞的，黑客就是透過尋找不同漏洞來入侵企業的系統，這時防守一方能否及時發現問題，並迅速加以對應及修補漏洞，將是能否擋下攻擊的關鍵。

由偽裝成可靠網站的偽冒網站攻擊、引誘點擊的釣魚電郵、近年大為流行的勒索軟件，以至針對特定企業客戶而設計的攻擊 - 持續性滲透攻擊（APT），黑客攻擊實在日新月異，中小企往往難以預防，尤其APT攻擊往往沒有任何前例可參考，隨時被攻擊了仍懵然不知。

為了應付這些愈來愈難提防的新型入侵式病毒，「沙盒」技術自然少不了。「沙盒」技術是指各種檔案會先在受監控的環境打開一遍，再觀察是否有可疑行為出現。而中信國際電訊CPC的托管式安全解決方案則更進一步，其TrustCSI™ Secure AI解決方案引入機器學習和人工智能，透過分析學習一般軟件和惡意軟件的行為，尋找更多特徵來分辨可疑網絡活動，以進一步打擊黑客。

除了APT攻擊，針對物聯網的攻擊也日漸常見。智能設備廠商未必在設計時考慮到資訊安全問題，在技術良莠不齊的情況下，這些設備都很易成為黑客攻擊的接入點。黑客會利用這些裝置連接到企業的內部網絡，或是成為殭屍網絡的一部分，很多時都成為IT保安的盲點，難以被發現。

中信國際電訊CPC亦留意到這些趨勢，其完整的托管式安全解決方案包含各種防火牆、網絡監控等，若發現有裝置連到不正常的網域或IP，或是出現不尋常的高流量都會盡快通知客戶，以阻止可疑的連線繼續執行，從而防止物聯網裝置成為黑客攻擊的跳板。而中信國際電訊CPC亦提供24 x 7的在地支援服務，並在發現可疑入侵時主動向客戶通報，迅速提供咨詢及建議，從而盡快堵塞漏洞。

中信國際電訊CPC資訊科技高級經理鄧志明指出「單靠傳統方式來阻止黑客入侵愈見困難，因此通過機器學習和人工智能，就能透過了解用戶習慣，對比常見的黑客攻擊行為模式，可更快找出可疑的網絡活動。未來我們也會與更多國內的資訊保安品牌合作推出新服務，結合業界資深的資訊保安經驗，強強聯手來為客戶提供更強大的保護。」 SMB