TREND MICRO 趨勢科技

# 趨勢科技NVWE－日盛金控的網路戰友

日盛金控資訊處資深經理
許志偉

公司簡介：日盛金控，前身為日盛證券，位居全台歷史最悠久的金融團體之一。日盛金控自1996年上櫃以來，以穩定獲利為集團目標，持續實踐對投資人的承諾。成立於1960年的日盛證券，為日盛金控中最早成立、也最具代表性的事業處。

## IT部門：成本或利潤中心?

對許多產業來說，IT部門也許是個花錢單位，能省則省，但對金融業而言，IT部門除了預算支出，也能創造利潤，從金融業IT預算一向位居各行業之首，可見端倪。每年集團IT預算以億為計算單位的日盛證券，也不例外。

1996年開始架設企業內部Internet的日盛金控，以洞燭先機的眼光在1997年開始啟用微軟Windows平台，在其他銀行都用Unix的年代，日盛金控比其他金融單位早一步透析未來的趨勢。

## 金融IT生存準則：迅速反應

「日盛IT的補給線很單純，機房裡面全部都是Wintel的Server，補給線單一化的好處是公司反應比較快，遇到意外狀況，你要找人才及資源都非常快；因此我們從那時（1996）就跟微軟及Cisco建立非常好的Partnership。」日盛金控資訊處資深經理許志偉回憶。

百分之百的電腦都架設在微軟的平台上，日盛證券在前幾年蠕蟲病毒猖獗時，與其他金融單位一樣深受其害；即使當時已經使用電信等級的防火牆設備，仍抵擋不住惡意程式的入侵。經過與市場上其他產品比較後，日盛選擇了趨勢科技提供的一款主動式疫情防制硬體設備：NVWE（Network VirusWall Enforcer），過去Call Red時動輒48小時在辦公室待命的日子不再。

「過去抓病毒最久花一天，現在是立即解決，Response時間很短；因為建立了自動化的Reaction，若判斷這個行為確定是非法入侵，NVWE就直接Block掉，Procedure都定義好了，照這個來執行。」許志偉表示。

## 變，是不變的原則

同時具備偵測網路型病毒及防範混合式攻擊行為的NVWE，最近這幾年因為病毒型態改變，功用重新定義；針對未符安全規範的網路節點（Endpoint），NVWE採取NAC（Network Access Control）機制。除仍協助日盛IT人員防制網路病毒及蠕蟲，確保重要機器正常運作外，無論發現任何來自網路節點上的安全弱點，NVWE都能自動修補漏洞（如補上微軟Patch）；即使不幸遇到疫情爆發，NVWE也能隔絕高危險的網路脆弱環節，遵循已定義的安全防制策略，並在缺乏防毒保護的裝置等潛在感染源連接網路時，予以隔離和清除。

「因為NVWE的代理程式（PE Agent）種在每一台Client端，我們利用PE Agent去撈Client端的機碼（Registry），裝什麼東西都可以透過NVWE看得到；甚至可以做到只要Client端沒有裝防毒軟體，一律無法上網。」許志偉仔細解釋功能的重新定義。

- 主動式的疫情防治系統　讓企業免於惡意程式威脅
- 有效的病毒及安全弱點偵測　企業網路使用更安心

## 金融IT的核心價值：客戶滿意度

金融業的競爭力來自於客戶滿意度，而金融業IT的核心價值在於創造客戶滿意度。日盛金控目前有1000台電腦分別受到10台NVWE的保護，主要是針對後台行政人員所接觸到的機台資料；未來希望把應用範圍擴大，增加1000台以外的PC數，除了延伸到公司其他單位外，也預期能提供客戶端資安應用程式，保障重要客戶在家及辦公室的交易安全。

「金融業IT的核心價值在服務內外部的客戶，除保障外部客戶資料的CIA（Confidentiality, Integrity, Availability）外，也對內部客戶即員工提供BCM（Business Continuity Management），讓業務持續進行，服務不中斷。」許志偉總結。

詳細產品訊息，請上趨勢科技網站
NVWE：www.trendmicro.com.tw/nvwe.htm
申請免費試用，請洽詢趨勢科技服務專線：(02)2378-2666

TREND MICRO 趨勢科技