保護個資　內網安全防禦之首要

面面俱到的使用者控管機制

如標題所述，內網安全防禦之首要在於做好使用者控管機制，其重點就在【如何偵測與判別使用者身份】與【事件產生的防禦工作】是否能夠滿足現行網路環境的需求與徹底解決問題的能力。

複合式的網路存取環境 應採多重身份識別認證

專精於研發內網安全網管系統的NetAxle公司總經理葉華裔表示，傳統用IP+MAC單一鎖定方式已經不敷使用，所以NetAxle特別開發一多重使用者識別認證，可配合企業的需要選擇IP+MAC鎖定、MAC認證、WEB認證、與搭配DHCP應用的交互多重認證，可完全滿足企業不同環境的需求。

內網安全偵防 不容一絲破綻

市面上許多廠商採用以攻擊的手法來回防駭客，在Internet上就可下載各種不同的攻擊工具，例如採用DNS Hijack攔截非法使用者的DNS Query封包，將其重導致告警網頁並顯示告警訊息；或是採用ARP Spoofing持續對非法使用者送出ARP封包干擾，但是以上2種方式都存在極大的防禦漏洞：駭客都還活在內網裡！前者不一定攔截得到駭客unicast的DNS Query封包，而且必需在合法DNS Server回應前先送回假冒的DNS Reply封包，若DNS Hijack主機效能稍差，延遲個0.1秒就攔截失敗。後者若遇上駭客使用同樣的ARP Spoofing程式，發送了10萬筆假冒的ARP封包要影響或攻擊網路，則防禦機制會自動以ARP Spoofing反擊回去並送出了100萬筆反擊封包，若遇到聰明的駭客故意不斷發送此類封包而不攻擊任何主機，則網路反而會因為防禦機制啟動暴增的反擊封包而陷入癱瘓了。

應用SNMP建立防禦網 預防與阻絕攻擊的漫延

葉華裔總經理強調，Switch Port Shutdown可說是最安全的防禦機制，唯有應用SNMP模式，與Switch設備互相配合，將內網包含Layer2以下的每個端點都找出來，透過集中控管的方式下達指令，才能快速阻擋攻擊漫延甚至將之殲滅。葉華裔總經理表示，NetAxle研發的NetIRS系統因偵測與防禦都採用SNMP機制，可以精確的辨認每個Switch埠連接情況，進而達成Switch Port Shutdown，徹底將駭客殲滅，建立堅強的防護網。

支援IPv6以因應未來 現行對策：回收IP與 Switch Port！

今年6月國際網路學會(ISOC)贊助成立World IPv6 Day，目的為協助企業做好IPv4轉換到IPv6，所以因應未來個資法防禦的內網偵防設備也必須支援IPv6。葉華裔表示，NetIRS不但支援IPv6，對現行IPv4為防止IP不夠用的問題，提供回收閒置不用的IP與Switch Port，讓閒置的IP能善加再利用，也避免閒置的Switch Port被盜用增加管理的風險。

不僅逮捕　還可以

判

死刑

Switch Port Shutdown 最安全

駭客只要活在內網裡，100% 都會再犯
唯有應用SNMP模式，自動關閉駭客連接埠
才能徹底殲滅，無法再進入網路

真正保護個資　終結駭客認務

NetIRS 聯合防禦網管系統

台灣授權代理商

捷宇網安

力麗科技 LeaLea Technology
力麗科技股份有限公司
台北市松江路162號6樓
總公司TEL:02-2100-2458

特約經銷商

逸盈科技 NetFos Technology Corporation
逸盈科技股份有限公司
台北市八德路四段760號7樓
總公司TEL:02-6636-8889

豪勉科技
豪勉科技股份有限公司
台北市承德路一段70號3樓
總公司TEL:02-2559-6163