E-News

發行人：捷宇網安行銷部 發行日期：2011.10.3

●內網使用者控管不能只做半套

在我們解決客戶的案例中，最常碰到的問題就是其原本已購置的 IP+MAC 身份控管的產品，會因為網段與設備的擴充或變化而無法跨網段使用，並且還必須不斷購買端點的偵測器，反而增加管理人員的負擔，也不能對有問題使用者做嚴密的防堵。

◆ 使用者控管需囊括二大類別

然而我們認為，一套完整的使用者控管機制，其重點必須要能夠滿足現行網路環境的需求與徹底解決問題的能力，所以客戶可以依據其產品是否囊括以下二大類別來判斷符不符合貴單位採用：

一、俱備彈性的使用者身份識別與管理能力

二、在最經濟的模式下提供最嚴密的防禦

第一類別因案例冗長，留做下期 E-News 來探討，以下就第二類別—問題使用者的防禦工作，提醒管理者認識使用者防禦機制的原理。

◆ 認識使用者控管的防禦原理

市面上有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。

◆ Switch Port Shutdown 最安全

Switch Port Shutdown 可說是最安全的防禦機制，因為一旦攻擊者的 switch port 被關閉後，攻擊者已完全失去網路連線，當然不可能再攻擊網路。然而 switch port shutdown 有一些要求和限制需配合與小心使用：1、Switch 設備需支援 SNMP 功能，如此才能將 switch port 成功 shutdown；2、在 shutdown Switch Port 時需能避免關閉到不該關閉的 port，例如 Uplink port 等。現在 Switch 支援 SNMP 已不是大問題而且價格越來越平民；而 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 埠連接情況以及其 Uplink port，進而達成 Switch Port Shutdown，建立堅強的防護網。