新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2009/3/23- 2009/4/5 第88期

網路記錄器 / IR 系列報導

技術淺談與應用 - 如何選擇網路記錄器的三種記錄模式？

網路記錄器於目前資安設備中，早已經是個不可或缺的重要環節，在林林總總的資安事件不斷發生下，相信不少公司企業能夠深深瞭解到資安方面上各項記錄是最為重要的憑證依據。舉凡訊息傳遞、即時通訊、電子郵件…等，該如何將其內容一一記錄下來當作存證依據？如何避免網路的資源被濫用、洩密及保存公司重要的資料？網路環境越演越複雜，加上網管人力總是不夠用的情況下，選擇正確的網路側錄設備才能夠幫助網路管理者、企業經營者，以最精簡的人力及最少的時間下滿足記錄存證與資安方面的需求。

而這些記錄資料如要有完整的證據能力，就需要清楚標示該記錄屬於哪位員工所有，以下除了將大家所熟悉的 "By IP" 、 "By MAC" 兩種模式歸納整理出所適用的時機及需注意之使用情況外，也針對 "By AD Server" 模式做說明，讓管理人員能夠有效率的為公司選擇最適當的記錄模式。

By IP Addresses

適用時機：企業網路環境內部的使用 IP 都有固定分配。

注意：因為此種記錄基準是以每位使用者的 IP 為判斷條件，倘若使用者所使用的 IP 可任意作變更，或是所使用的 IP 為浮動式 IP（使用 DHCP）情況下，採用此種模式時較容易發生所記錄下的內容不易分辯該項記錄 IP 當時為誰所使用，導致誤判的情形增加。

By MAC Addresses

適用時機：此模式採用 MAC 為記錄基準，可有效避免有心人士任意變換 IP 逃避查緝的問題發生，若企業內部 IP 可由使用者隨意變更或不固定時(如：DHCP)皆可適用此模式。

注意：當企業網路內部有架設路由器時要特別注意的是，透過路由器傳遞的封包其 MAC 會被路由器之 MAC 取代，所以網路記錄器的記錄基準需要採用以 IP 方式記錄，才不會發生路由器後端使用者上網記錄錯誤的情況。

By AD Server

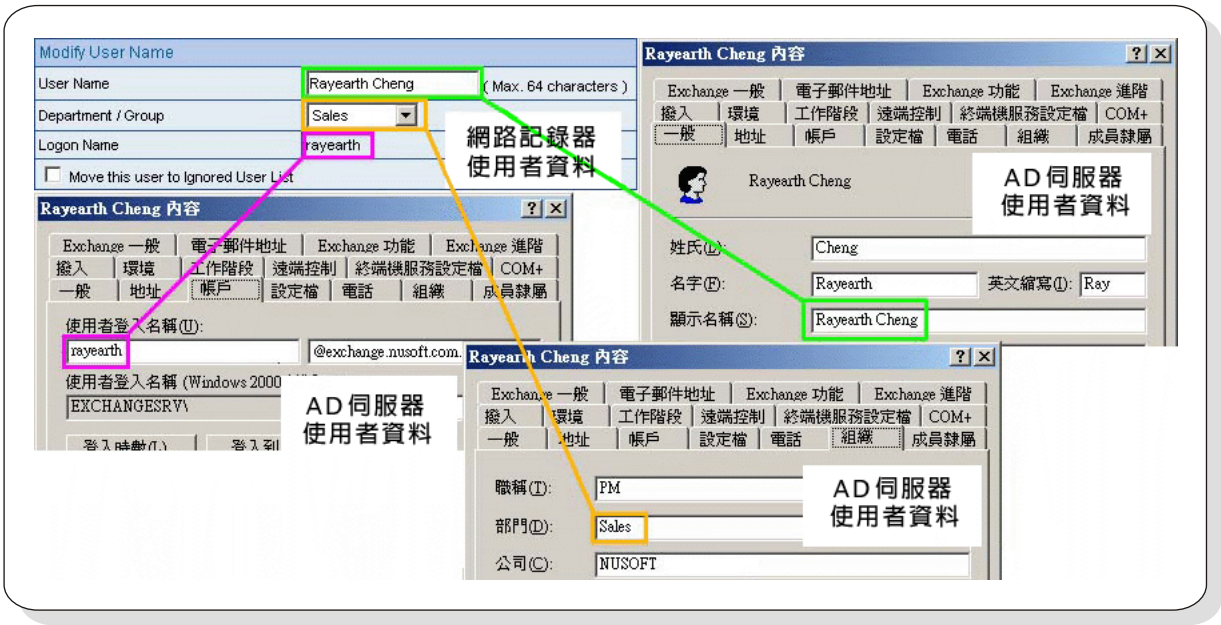
適用時機：企業內部若有架設 AD 網域時。

注意：需搭配系統中所另附之輔助程式 "IR Plug-in" 使用，利用 IR Plug-in 來統整結合 AD Server 上使用者的帳號資料。

好處：使用 By AD 模式後，能夠有效將其網錄記錄器之記錄依據結合企業內部所辛苦架設的 AD Server，即使是使用者名單有所變動時(如：新進員工、轉調部門、員工離職…等)，也只需要更改 AD Server 裡面的設定，網路記錄器-IR 上的記錄就跟著改變，完全不用管理人員再費時於機器設備上調整與變動。同時管理人員不需要再一個一個重新於 IR 中建立名單，在面對公司內使用人數較多情況下即可有效的節省掉不少設定時間與精力上花費。

	By IP	By MAC	By AD
適用環境	有固定分配 IP	IP 無固定分配	有架設 AD Server
注意	使用者可隨意變更其使用 IP 或 IP 為不固定 (DHCP) 時，不建議使用此模式。	若封包之傳遞有透過路由器時其 MAC 會被路由器之 MAC 取代，所以不建議使用此模式。	需搭配 "IR Plug-in" 結合使用。

記錄模式比較表



By AD 模式與 AD Server 結合圖示

文 陳殿鴻 kim@nusoft.com.tw

市場行銷報導 – IM 即時通訊內容採用「分離式對話視窗」方式記錄，讓資安管理更方便

在企業 e 化後，網際網路系統對企業的營運績效，有著不可取代的重要性。然而，方便的網路環境，除了能提昇營運管理的效率，背後也隱藏著資訊應用上的風險，諸如：客戶資料的保密、公司機密的洩漏…等等。因此資訊安全和管理稽核的結合已經是企業裡密不可分的重要管理政策。而方便的 IM 即時通訊工具是目前奔馳商場之重要武器，但是過於方便的使用已成為資安關注焦點。相關研究報告顯示，全球約有 30% 以上企業採用 IM 從事商業溝通，卻只有少數企業做到 IM 的管控。一方面藉著使用 IM 即時通訊而獲得便利性的同時，另一方面企業也必須積極運用管理工具來有效管控 IM 的使用。藉以避免發生如:員工趁機摸魚、公司機密外洩…等狀況發生。因此各企業對自己公司內部資安控管產生新的需求，尤其「網路資訊監控」、「收集」、「事後查詢」等相關需求，儼然成為目前各企業首要解決的重要問題。

而對「IM 即時通訊」做控管的最好方法，首推以「積極開放、有效管理」；依企業的網路政策決定何者方有權限使用即時通訊對外聯絡，再以網路側錄方式詳加記錄通訊內容，來替企業資訊安全把關。一般網路側錄設備的 IM 聊天記錄方式是採用「聊天室」方式記錄對話訊息；此種記錄方式雖然可以將員工的聊天內容逐條記錄，但是若員工同時與兩個以上之對象交談，則易導致聊天內容混雜。使管理人員在事後閱覽記錄時“很難確定該名員工此時到底是與誰在對話”的情況發生，造成管理上的不易。

因此新軟在所推出的「新軟網路記錄器」系列產品中，特別針對「IM 即時通訊」這部分，採用「對話視窗」模式來分類對話訊息，大大有別於其他市售產品；在其記錄表當中，不同對話視窗的聊天內容將分別記錄於不同筆記錄中。即使員工同時與兩個不同對象交談時，其交談記錄亦不會彼此混雜在一起，管理人員也能夠輕易了解所有對話內容。在新軟系統的網路記錄器裡，能使監控對象在記錄器下無所遁形，而且其具備便利、科學的檢索規則，能大大減少管理者分析記錄的時間，讓管理工作更方便、更有效率。

圖 1　透過 MSN，員工可同時與多人聊天

圖 2　一般網路側錄設備採用“聊天室”方式記錄即時通訊，易造成混淆。

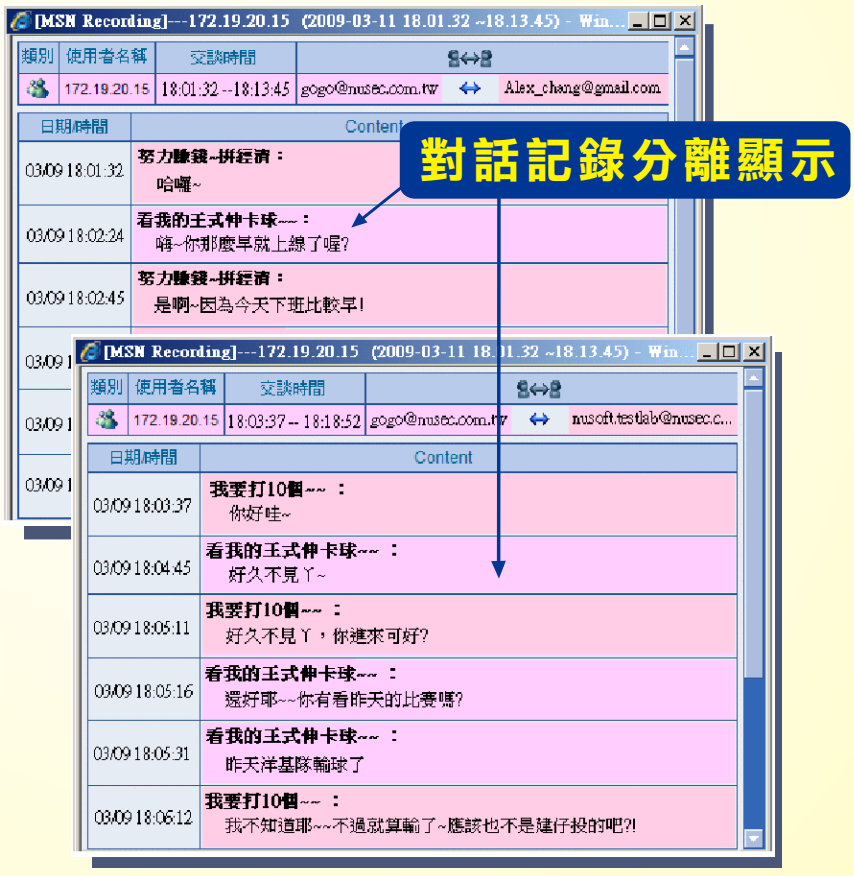


圖 3　新軟網路記錄器的記錄採用「分離式對話視窗」記錄機制

文 黃政銘 ming@nusoft.com.tw