產 業 報 導

強化資安管理 杜絕內部威脅

NetAxle 打造新一代網路安全統合系統

根據各種資安統計報告顯示，現在的資安事件有 80%來自於內部，從外部發起的攻擊反而並非主要影響企業營運的關鍵。但是過去傳統的資安防禦架構都是以外部攻擊爲主要假想目標，對於內部網路的控制與監控能力不足，也無法防禦內部的各種資安威脅。事實上在不影響營運效能的情況下，要能確保內部網路防禦是相當困難的事情，最好的方法就是強化內部行爲與各項資安事件管理。NetAxle 所推出之網路安全統合系統就是爲此目的而研發，藉由強大的管理與延伸能力協助企業強化內部資安事件管理機制。

近年來資訊安全越來越成爲企業關注的目標，除了因爲各種規範要求之外，駭客針對企業攻擊，以求獲得鉅額利益的行爲也越來越普遍，讓企業更是無從防禦起。細究其攻擊方式，內部攻擊的起源大多分爲木馬、蠕蟲或是內部不當行爲等，這些都不是一般資安防禦設備所能抵擋的，要能夠建構完整的防禦措施，第一步就應該要建立起有效的分析管理機制。

「各項資安設備所傳來的訊息與記錄都相當多，分析這些訊息對於管理人員來說是相當沈重的負擔，」捷宇網安總經理葉華裔表示，「最好的方式還是提供一套可以整合分析，且即時對異常流量及行爲做出回應的系統，如此才能簡化整體工作流程，讓管理更加簡單。」

防禦極端化攻擊方式

目前的攻擊行爲已經越趨極端，大多數攻擊都潛藏在合法行爲之中，單是仰賴防火牆、防毒牆或是 IPS 系統並沒有辦法檢測出真正的威脅起源，在沒有監控全局的核心設備之下，所有的設備只能根據自己所能負擔的環節，自行解決相關問題。「這項作法只是頭痛醫頭，腳痛醫腳的作法，最好的方式還是建構起整體網路安全控管系統，藉此建構全方面的安全防護，」葉華裔認爲。

而除了躲藏在應用層裡面的攻擊之外，另一項較難防禦的則是位居內部網路中的第二層攻擊。該攻擊會透過 MAC 層的諸多標準進行攻擊，不但可能影響重要的營運設備，更會讓癱瘓部份內部網路，而其攻擊的特性是其所影響的範圍都只局限在單一網段，但相對的也較難偵測出此類的攻擊事件，防火牆與 IPS 對此類的攻擊是幾乎沒有任何效用。

NetAxle 的 NetIRS 設備便是依據此一思考方向應運而生，此多功能網路安全平台能夠從其他資安設備抓取相關安全訊息，只要設備支援公開連接標準，如 SNMP、syslog、sflow 或 netflow 等，就可以將相關資訊送至 NetIRS 上，並透過該設備所具備的即時入侵反應系統（Intrusion Response System），進而建構企業內部的網路安全營運控管系統（NSOC）。

藉由完整且全面的資安控管機制，NetIRS 可以協助企業建構完整且簡易操作的安管中心，進而確保企業內部的資訊與網路安全，讓內部攻擊的發生率降至最低。

功能整合簡化資安架構

雖然建構完整資安架構可以協助企業打造良好的控管環境，但對於中小企業而言，多種設備不但需要花費高昂的成本支出，同時在維護管理上也需要消耗較多的人力資源。
捷宇網安方面認爲資安架構不應該只有大型企業才能夠建置，應該讓相關功能與效力可在中小型企業中落實，因此在 NetIRS 中，除了資安管理系統之外，更納入了防火牆、入侵偵測與流量分析器等功能。

「爲了降低中小企業對於成本與管理上的壓力，NetIRS 提供整合性的功能，」葉華裔表示，「透過軟體模組及穩定的硬體設備結合，能夠讓中小企業降低營運及維護上的困難，同時兼顧全方位安全管控。」

透過軟體模組能讓中小企業以較爲簡單的方式建構資訊安全，同時簡化網路拓樸的複雜性，管理上也更趨集中化。當企業規模不斷成長，除了可以快速更新設備與模組之外，亦可另行採購專業等級設備，以強化特定資安功能。NetIRS 所提供的功能不但多樣化，且延伸性與彈性良好，讓企業能夠依據自身需求而彈性建置。將不同功能整合在單一設備除了節能與簡化管理外，更重要的的是透過不同功能的整合更可將各自的資訊互相關連以提供使用者更立即清楚的完整資訊.

雙重專業打造加倍安全

捷宇網安的研發團隊多位於台灣，除了能夠強化研發能量並深耕台灣企業之需求外，同時也能加速滿足客戶的特殊需求。

「客製化是台灣企業相當重要的需求，因此我們將研發中心集中於台灣，」葉華裔表示，「這樣才能讓我們與客戶得以緊密連結，提供更快更確實的服務。」

此外，在銷售上也與逸盈科技合作，透過逸盈科技長久以來在企業界耕耘的成果，共同將產品帶入企業之中，搭配上眾多系統整合業者協助，能夠讓企業以最佳解決方案方式導入 NetIRS，一方面避免疊床架屋的架構，另一方面也以更切合需求的方式提供產品與服務，讓中小企業能在金融風暴之後快速恢復，且建立更安全穩定的網路。更多資訊請洽代理商逸盈科技 (02) 6636-8889 或至 www.netfos.com.tw 查詢。