

Exchange 夠安全嗎?!

『若沒有強大的安全性，您的協同作業環境就像敞開大門般等著被人入侵…』

爲何需要安全性？若沒有強大的安全性，您的協同作業環境就等於如同敞開大門般等著被人入侵，換言之，您的企業機密就如同攤在陽光下一覽無疑，再想想，哪您的企業資產是否全然失去保護呢？。ICSA 實驗室的病毒盛行調查，「…透過電子郵件傳播，仍是電腦病毒散佈的主要方式」。此外，從病毒事件中進行完整復原的平均時間是 31 天，從單次病毒事件中復原的平均花費超過 130,000 美元。此外，所有的理由都足以讓您相信，以後情況可能會更糟。2005 年 6 月在 MessagingPipeline 上的一篇文章，列出 Radicati 根據電子郵件與電子郵件安全性所做出的幾項預測，未來將有數百億至上千億封電子郵件蓄意攻擊或散佈病毒流竄各地。

駭客每每使用電子郵件作爲入侵企業系統竊取機密資訊的入口。2005 年 6 月，MasterCard International Inc. 在信用卡交易公司 CardSystems Solutions Inc. 發生了安全性入侵事件。CardSystems 被狀似病毒的電腦指令碼攻擊，這類的指令碼通常透過電子郵件傳送，客戶資料遭到竊取，可能影響 4 千萬名 MasterCard 持卡人。

這類的入侵可能讓企業名譽蒙上污點、損失客戶，甚至惹上官司。此外，在有些案例中，資訊安全是明文規定的，如歐盟資料保護法、美國健康保險流通與責任法案等等，以保護病患資料。這些法規同時要求企業擷取、儲存並產生電子郵件和即時訊息，以證明遵守安全性政策。若未遵守這些法規的會導致罰款。

爲了解決像這類的協同作業困難，您必須了解，安全性必須是原本就存在，而不是後來再附加上去的。除非在產品設計過程中就考慮到安全性，否則該產品都只能對衍生問題做出反應，而無法主動預防。這無疑對 IT 人員而言是一大負擔。想想，微軟爲修補 Outlook/Exchange 上新發現的弱點，得不斷發行新的安全性修補程式。而企業爲求保護重要的系統與機密資料，必須亦步亦驅地執行這些修補程式，這需要投注多少的人力與預算啊。

此外，資料加密也是安全性考量之一，這樣，一但資料被盜也無法解讀；另外，在應用程式編寫介面 (API) 的層面，除了爲協力廠商開發人員建立存取權，同時仍需保有應用程式的安全性。

如果您是Exchange的使用者，過去的屢次中毒受駭經驗可能已讓您發現，病毒與病蟲會透過 Outlook 中接受 ActiveX 與 Visual Basic 的特性，輕鬆進入 Exchange，這無異是敞開大門接受代價驚人的破壞性病毒攻擊，而不顧資料安全。相反的，另一套優異的產品Novell GroupWise 從設計之初就一直將安全性銘記在心，以確保整個系統（包括郵件儲存庫）不受病毒與病蟲攻擊。

GroupWise 也能保護不受垃圾郵件騷擾，這同時也是病毒入侵的來源之一。它提供多層級的防垃圾郵件控制，GroupWise Internet Agent 與用戶端會保持郵件儲存庫無毒，並可減少員工花在刪除垃圾郵件的時間。

但光是電子郵件做好防護還不夠，公用 IM 即時通訊也是易受攻擊的地方。同一層辦公室中兩個員工互相傳送的郵件，其路徑並不只在這個辦公室而已。該郵件會橫越網際網路 – 可能還會跨越數千哩。這些通訊可能會被輕易攔截，讓您的資料遭竊。GroupWise 不會讓您的訊息公開的在網路繞行，因為您使用的是企業專屬的 GroupWise Instant Messenger。此外，SSL 與專利的 Novell 加密安全通訊，和順暢的資料儲存庫搜尋功能，可迅速回應公司或法律對電子郵件或 IM 副本的要求。

我們都了解，結束一段關係可能會很難，但總有一些人、一些事，是您等不及要擺脫的。舉例而言，試想揮別具有業界最糟病毒記錄的協同作業系統、甩掉過多的當機時間與復原費用等等。當您安裝具有卓越安全性與可靠追蹤記錄的協同作業系統時，一切的感覺會多麼美好！若您是Exchange使用者，且正在尋找更安全、可靠、適應性高的郵件平台，Novell 向您推薦 Exchange 客戶的最愛 – GroupWise，現在您可以痛快地向全世界最不安全的協同作業系統說再見了。

	欲了解更多有關Novell GroupWise 的訊息請造訪 http://www.novell.com.tw/groupwise/seminar/
	GroupWise 體驗專線 0800 012 335