雲端拓展新疆界(上)
-軟體安全如何解放雲端運算的力量

研究摘要

雲端運算在 IT 領域獲得了極大的關注與迴響。無論在節省成本、靈活創新或是即時容量管理方面，都驅動許多企業內 IT 組織將部署雲端的策略納入計劃之中。雲端運算的好處，須取決於可信的雲端運算基礎設施－特別是控制私有數據（private data）和關鍵流程自動化的軟體。而近來網路威脅已轉向應用軟體層面，IT 組織不僅必須涵蓋優化雲端部署的軟體，且須限制靈活性，並能節省花費。因此，若要解開雲端運算的力量並實現其最終利益，維持固有的安全軟體保證是一個關鍵。本文描述了上述概念以及佈署後對有興趣移動到雲端的機構、消費者、和雲端服務的提供者的利益。

雲端運算的好處

因企業和政府不斷尋找節省成本和提高業務靈活性的產品，故雲端運算在企業和政府機構是非常受歡迎的。根據產業研究公司 IDC 以複合年增長率調查結果，雲端運算約有 27%增長軌跡，成長速度是傳統部署模式的五倍。雲端服務業務增加了 25％，若以同樣的軌跡繼續成長，2013 年以前，雲端服務會使 IT 行業產生大約三分之一的淨額成長。(資料來源: 《*Worldwide IT Cloud Services Spending, 2008-2012, IDC, October 2008*》)

雲端運算從業人員列舉了許多雲端的益處，但在多數情況下，有兩項基本效益：

- **即時性：**企業能在極短的時間內得到運算資源，僅需極少成本即可佈署解決方案，並可隨時暫停或中止服務。IT 部門不需投資前置網路、硬體或儲存設備，即可自由擴充或縮減其生產／需求能力。此外，使用者不需在辦公室也可任意地存取資訊。
- **降低成本：**雲端運算費用計算模式乃根據消費和利用共享的基礎建置的程度。供應商可以將成本攤在多個客戶之中，故公司只須支付使用費用即可。雲端運算不僅能延後 IT 基礎設施建置，也可自由擴充或縮減投資項目。不用 100%擁有專屬的基礎設施，亦可大量節省成本。

其它效益包括協同作業、擴展能力與高可用性等；但企業大量採用雲端技術的主要因素，不外乎大量節省成本及其即時性。

GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

何謂雲端?

截至目前為止，許多文章、廣告或討論區皆充斥雲端運算的議題，但若要達成共識，仍須定義「雲端」一詞。一般來說，雲端運算指透過網際網路進行擴充、消費或提供 IT 服務，因此顧客可隨時取用 Web 化的網路資源、軟體或資料。正是這種共享及標準化概念形成雲端的核心價值。透過雲端運算，供應商可將成本分攤到許多客戶，亦即，這些成本也會反饋於客戶本身。轉移分攤運算基礎設施成本是一個合乎邏輯的典型副產物，也會產生易於存取於網際網路上的遠程站點和虛擬運算站點的概況。

美國國家標準與技術研究院（NIST）定義了四個雲端部署模式：

1. **私有雲（Private Cloud）：**該雲端基礎設施被單一個組織擁有或租賃，而且是專供該組織運作。
2. **社區雲（Community Cloud）：**該雲端基礎設施被多個組織所共有，並且支援擁有共同議題，而這些社區雲更應該考慮安全需求。
3. **公有雲（Public Cloud）：**該雲端基礎設施被某企業以雲端服務方式銷售至一般公共或大型產業組織。
4. **混合雲（Hybrid Cloud）：**該雲端基礎設施由兩種或兩種以上的特定模式組成的組織運作，但可藉由標準化與專屬技術來使數據和應用程式方便移植。

NIST 對雲端的定義不僅僅是如何共享基礎設施，也包含了共享哪些元素。這些服務模式移轉了使用者與供應商之間的安全責任：

軟體即服務（SaaS）：為最成熟的雲端服務。SaaS 提供完備的環境，透過瀏覽器可依客戶個別需求即時使用一般的應用程式。通常情況下，客戶不需多費神，僅需設定用戶即可。安全方面完全受控於供應商。此類供應商的案例包括：Salesforce.com、Workday、Mint.com 以及其它數以百計的廠商。

平台即服務（PaaS）：為新興的雲端服務模型。客戶可在其平台上使用供應商提供的程式語言與開發工具軟體，或將軟體部署在雲端的基礎設施，但無法控制實體的基礎設施－如網路、作業系統、伺服器或儲存空間。因為客戶控制應用程式的設定與開發，因此安全責任大部份移轉至他們手上。此處供應商的案例如：Google App Engine、Amazon Web Services…等。

基礎設施即服務（IaaS）：此處的特徵是基礎設施的多租戶使用情況。雲端服務供應商提供運算力、儲存空間、網路以及其它基本運算資源。客戶可以部署或執行任意軟體，包含作業系統與部署的應用程式。在此部署模型下的軟體安全完全在客戶的手上，包含防火牆等元件。此處供應商的實例如：Amazon Elastic Compute Cloud、Rackspace Cloud……等。

正當 SaaS 成為許多組織內部軟體的替代品時，PaaS 和 IaaS 也大量驅動業界對雲端運算的興趣。PaaS 和 IaaS 所提供的「替代研發基礎設施（alternative development infrastructure）」和「資料中心策略（data center strategy）」特別吸引多數企業。在這點上，小型企業似乎與 PaaS 有較多關連，它能使 Web 網站可以更快推向市場上；但更大型的企業需要把他們既有的應用程式推向 IaaS 的雲端模型之上。

GSS Galaxy Software Services 叡揚資訊 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

「雲端運算可減少組織花費並增加運算方案的彈性。然而，若要完全理解這些效益，客戶必須承認基礎設施有其弱點，亦即愈來愈多針對軟體的網路威脅，不該侵入雲端共用服務或者提供給駭客新的存取私人資訊通道或干擾商業處理。」

雲端安全聯盟董事會主席暨共同創始人 Dave Cullinane

雲端內的軟體安全

現今駭客及惡意使用者有充份理由以攻擊軟體為目標：軟體可控制流程、儲存媒體及使用資料，且容易攻陷。產業分析師估計駭客攻擊中有高達 75%是在應用軟體層。此外，現今的應用軟體非常複雜，從研發、部署與上線過程的安全保護措施不像網路或硬體設施那麼成熟。應用程式放置在共用的雲端環境，而軟體複雜度不斷攀升，如同把額外的壓力放在這個脆弱的線上安全的連結上。

由於上述原因，無論雲端運算服務的形式為何，軟體安全已成為關鍵因素。利用 NIST 所指出的 PaaS 與 IaaS 服務模式時，SaaS 服務模式是一個特例，商業和政府機構更需要拉出額外的控制才行（請參考第二十期「企業資安指南 SaaS 軟體即服務的安全性」一文）。無論是何種模式，軟體安全皆適用於所有放上雲端的軟體或應用程式。因此，「雲端冒險」前，組織需要確保使用的應用軟體已經「雲端就緒」。

企業應用程式往雲端邁進時，需檢視一些開發人員假設的狀況，結果為何，影響甚大。底下幾項範例可以協助發現潛在問題：

1. **傳輸通訊協定：**以往，應用程式若僅供內部使用，即使用 HTTP 通訊協定也不太有風險；但是同一朵雲若轉往公眾網路時，相同的協定就會產生新的問題。撰寫軟體時若已納入安全議題，即可輕鬆應付變更協定這件事情；但是軟體設計若太差勁，想要輕鬆應付，恐怕很困難。

2. **網路基礎設施：**典型的資料中心在 IT 部門控制下提供資源。例如：DNS 伺服器提供了「黃頁」作為電腦間方便互相找尋的媒介。現在軟體移至雲端，倚靠的是公眾 DNS 伺服器。所造成的結果是：網路罪犯多了一個新的攻擊機會。

3. **資料保護：**組織內部假如以個人資料來記錄日誌檔，內部仍可輕易管理資料洩露的層級。而在雲端，因為無法掌握管理人員，因此只要是個資會出現的地方，即須更嚴謹地控管。

目前雲端軟體安全的方法

下期待續…

GSS Galaxy Software Services 叡揚資訊 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787