

網絡安全威脅分析

(雲端服務)

第三組



1.1-1.2雲端服務的 威脅/來源：

當帳戶遭入侵，攻擊者通常會使用網路釣魚活動來竊取員工密碼，並取得系統和重要公司資產的存取權。硬體和軟體弱點：無論組織使用的是公用還是私人雲端，安裝硬體和軟體的修補程式並保持在最新狀態至關重要。而在內部威脅，人為錯誤是造成安全性缺口的一大原因。

1.3雲端服務的 嚴重程度和可能性：

雲端出現安全漏洞時，公司都會在試圖恢復時損失金錢、時間和資源。雲端漏洞所導致的停機可能造成嚴重的營運挫敗——雲端中的應用程式和資料，以及與雲端連線的裝置和網路可能會暴露於許多威脅中。

1.4針對每種雲端服務威脅的對策威脅的可能性：

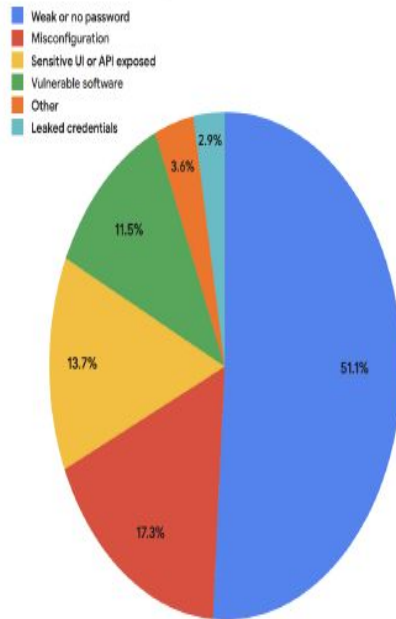
為了應付雲端服務威脅，雲端安全機制是一組網路安全措施，用途是保護雲端應用程式、資料和基礎架構，主要是透過實行安全性政策、做法、控管措施，以及身分與存取權管理和資料遺失防護工具等其他技術，來協助保護雲端環境，防範未經授權的存取、線上攻擊和內部威脅等問題。

2. 雲端服務威脅分析

重點: SSH 及 RDP 上的脆弱密碼是導致雲端服務遭受攻擊的主因

根據 Google 所做的資安事件統計, 超過半數的雲端入侵事件起因於 SSH 或 RDP 等遠端通訊協定設置過於脆弱的密碼或根本沒設定密碼, 駭客得以輕鬆獲取企業的雲端平台權限, 進而濫用其雲端資源於挖礦等用途。

- 攻擊類型: 阻斷服務攻擊 (DOS)、憑證外洩、暴力攻擊 (Brute-force attack)



3.雲端服務安全問題來源

雲端環境承受的安全性風險和傳統環境可能會發生的問題類似，例如內部威脅、資料侵害、資料遺失、網路釣魚、惡意軟體、分散式阻斷服務攻擊和 API 有安全漏洞的情況。

不過，大多數機構都有可能會遭遇特定的雲端安全性難題，包括：無法掌握情況、設定錯誤、存取權管理、變動不定的工作負載和法規遵循

雲端安全檢查表

檢查項目

- 1.實體及邏輯網路的屏障
- 2.端點的存取控制及管理
- 3.非密碼認證機制
- 4.憑證的質量控制
- 5.密碼重設的流程與機制
- 6.即時的異常檢測
- 7.事件日誌的完整度與備份、分析

資料來源：DIGITIMES，2010/10

4.雲端安全問題

在過去12 個月內經歷過安全事件的雲端用戶中，19% 的事件涉及錯誤配置的資源或帳戶。由於特定於提供者的配置設定範圍廣泛，錯誤配置仍然是雲端資安的重大挑戰。不熟悉雲端環境的公司及其員工可能會意外地錯誤配置這些設置，使雲端環境容易受到攻擊。多雲端環境的盛行加劇了這個問題，公司必須為多個不同的雲端供應商正確配置設定。

七個移動到安全雲端環境的注意事項

如何成功並安全的轉移到雲端環境，讓企業網路和管理能跨越整個多雲結構，達成一致性的架構

