新北市教育局雲端網域市集

風險評估

2010年發布的 Google Workspace Marketplace 是一個應用程式市集線上商店，其中具有企業級的應用程式，幫助雲端原生應用程式增加更多功能。管理員透過瀏覽、採購和部署企業級的整合式雲端應用，而開發者則可以在此應用程式市集中開發應用，進而銷售應用和服務。

管理員可以允許使用者安裝應用程式市集中的應用程式，請注意這麼做有可能會增加資料外洩、資料竊取及遭受惡意內部攻擊的風險，Google 不會為此事做任何擔保。
https://support.google.com/a/answer/7491894

資料竊取

「資料竊取」意指未經授權而將資料複製或轉移至網域外的行為。這類資料轉移可能是由具備機構內部資源存取權的使用者手動進行，或是透過網路中的惡意程式碼自動執行。舉例來說，資料遭到竊取的原因可能是具備資料存取權的帳戶資料洩漏，或是裝置上安裝的第三方應用程式將資料傳送至網域外。

資料外洩

「資料外洩」意指未經授權而將機密資料轉移至網域外的行為。資料外洩的途徑可能是電子郵件、視訊、雲端硬碟、群組或行動裝置，外洩原因則可能已含惡意或非惡意行為，例如啟用群組的公開存取權、採用意數的雲端硬碟共用設定、行動裝置遺駁，或是經由外寄電子郵件的附件外洩。

資料刪除

「資料刪除」意指惡意刪除資料而導致資料難以還原或無法還原的行為。舉例來說，攻擊者可能會植入勒索軟體將您的資料加密，然後要求您付款換取可解密資料的金鑰。

惡意內部攻擊

「惡意內部攻擊」意指貴機構內通過核准的使用者或管理員惡意將機密資料洩漏給網域外部人員的行為。惡意內部攻擊可能來自員工、離職員工、承包商或合作夥伴，資料外洩的途徑則可能是行動裝置遭到入侵，或是有人透過電子郵件將資料內容傳送至網域外。

帳戶資料洩漏

「帳戶資料洩漏」意指未經授權而存取網域內使用者或管理員帳戶的行為。帳戶資料遭到洩漏是因為未經授權的使用者竊取登入憑證。在這種情況下，攻擊者會將您網域中遭洩漏的帳戶資料做為他用。魚叉式網路詐騙是竊取憑證的常見方式之一，也就是駭客會假冒您認識或信任的個人或企業向您傳送電子郵件。

權限提升

「權限提升」意指攻擊者成功入侵您網域內一或多個帳戶，並嘗試運用有限權限取得權限層級較高的帳戶存取權。這類駭客一般會嘗試取得全域管理員權限，藉此全面掌控您的網域資源。

密碼破解

「密碼破解」意指運用特殊軟體和高效能運算技術還原密碼的程序，攻擊者會在短期間內嘗試多組不同的密碼組合。防止密碼破解的方法之一，就是對網域內的使用者和管理員強制執行兩步驟驗證功能。當 Google 偵測到帳戶有可疑活動時，也會封鎖帳戶。

網路詐騙或商業郵件詐騙

「網路詐騙或業郵件詐騙」意指假冒知名公司的名義寄送電子郵件，藉此誘導使用者提供個人資訊（例如密碼和帳戶號碼），或取得網域中使用者帳戶的控制權。網路詐騙分為以下三種類型：

- 網路詐騙攻擊：針對大範圍目標的電子郵件（大量寄送低成本郵件給許多使用者）。這類郵件可能已含網站連結，誘導使用者前往網站註冊來贏取現金獎勵，而受害者就會在註冊過程中洩漏自己的登入憑證。
- 魚叉式網路詐騙攻擊：針對特定使用者的目標性攻擊。舉例來說，某位會計師開啟安裝惡意軟體的附件後，該惡意軟體協助攻擊者取得會計和銀行資料。
- 商業郵件詐騙攻擊：試圖誘導使用者進行特定操作（例如匯款）。商業郵件詐騙會偽裝成正規機構所寄出的重要業務電子郵件。

假冒

「假冒」意指攻擊者藉由偽造電子郵件標頭假冒成其他寄件者，讓使用者無法得知電子郵件的真實來源。當使用者看到電子郵件寄件者時，會認為郵件來自認識的親友或是信任的網域。當電子郵件使用者相信郵件來自正規來源時較有可能開啟郵件，因此電子郵件假冒是網路詐騙和垃圾廣告活動常用的手法。

惡意軟體

「惡意軟體」是基於不良意圖設計的軟體，例如電腦病毒、特洛伊木馬程式、間諜軟體和其他惡意程式。

商業行為

「商業行為」任何形式的商業廣告、商業活動等進入中小學和高中職，可能會扭曲教育的本質，影響孩子身心健康。

審查與分級

「審查與分級」由於涉及未成年用戶，本手冊無建立審查與分級判度之規範。