確保第三方 API 安全的五個最佳實踐

應用程式介面（API）已經成為設定功能和彈性不可或缺的一部分。但是它們也是潛在的攻擊媒介，所以必須是安全團隊務需保持高度關注的重點。

文／Linda Rosencrance　譯／酷魯

當企業組織考慮到 API 安全性時，他們通常關注於保護內部編寫的 API。然而，並非公司所使用的所有 API 都是內部開發，有些是由其他組織設計和開發。問題是，許多公司沒有意識到使用第三方廠商 API 有可能會使他們的應用程式出現安全問題，例如惡意軟體、資料外洩和未經授權的存取行為。

第三方 API 是允許組織在自己的網站或應用程式上運用第三方功能或資料的軟體介面。技術研究和諮詢公司 ISG 網路安全總監 Phil Quitugua 表示，這些第三方 API 讓開發人員能夠將他們自己的應用程式或系統與外部服務、資料或功能整合在一起。

一些流行的第三方 API 包括導航 App、社交媒體平台和數位支付處理工具。「這些由 Google 或 Facebook 等第三方廠商提供的 API，讓你可以在自己的網站或 App 上存取他們的資料或功能，」AI 防護網路安全公司 DataDome 產品副總裁保 Paul Scanlon 表示。「每個人都喜歡 API。透過使各種裝置和應用程式能夠透過各種通訊協定交換資訊，API 可以協助開發人員更輕鬆、更有效地創造出色的使用者體驗。」

但在 API 無所不在和廣受歡迎的同時，潛藏著一個安全上的致命弱點 — 根據 API 安全平台供應商 Salt security 發佈的《2023年第一季度 API 安全狀況》（State of API Security Q1 2023）報告指出，在過去的一年中，大約 94%的公司在開發製作 API 的過程中遇到了安全問題，有 17% 的公司遭遇了 API 相關的資料外洩事件。因此，我們需要落實第三方 API 的安全性。

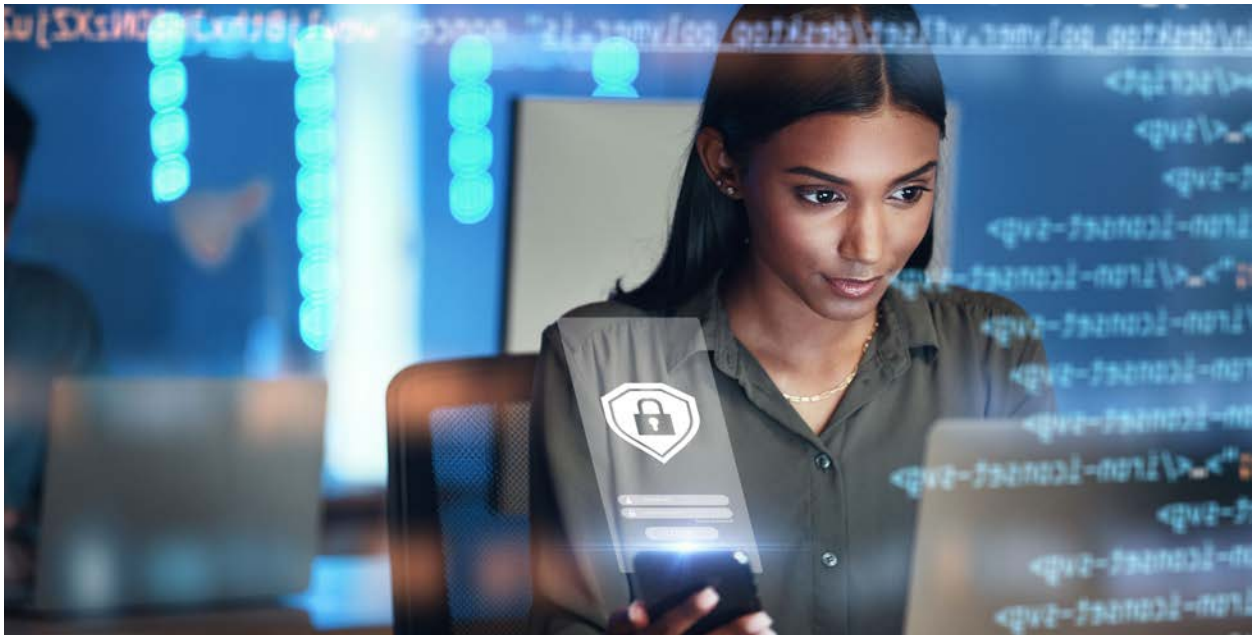
為什麼確保第三方 App 安全如此重要

安全服務公司 NCC Group 工業和營運技術業務總監 Jim McKenney 表示，第三方 API 需要強大的安全性，因為它們本身可能是安全弱點。如果它們不安全，它們可能會洩露敏感性資料或導致原始軟體出現問題。

「API 安全能夠保護程式之間的通訊免受網路威脅的危害，例如開放街圖（OpenStreetMap）所提供的 API 便是如此，」McKenney 指出。「它可以抵禦惡意攻擊、未經授權的存取行為以及 API 濫用等新興安全威脅。API 安全確保了應用程式之間既安全又可靠的交流。」

凱捷管理顧問公司（Capgemini）旗下 IT 服務供應商 Sogeti 洞察和資料副總裁 Doug Ross 表示，第三方 API 安全涉及認證、授權、加密和監控等實施辦法，以確保 API 及其資料的隱私性、完整性和可用性。「API 安全是軟體開發上的一個關鍵面向，因為 API 經常充當不同系統之間的橋樑，而且愈來愈頻繁地用於交換敏感和關鍵資訊，」Ross 說。

基於許多原因，確保第三方 API 的安全性非常重要。因為一方面，API 可以存取敏感資訊，例如使用者資料或支付資訊。因此，一旦第三方



API 遭到入侵與劫持，那麼就有可能導致資料外洩，進而對終端使用者以及依賴 API 的企業造成影響。此外，不安全的 API 可能會使應用程式或系統置於漏洞和攻擊等安全風險之下，進而可能造成系統失效或資源不當存取等狀況的發生。

第三方 API 的安全性在維護合規性方面也很重要，因為許多產業都有嚴格的資料保護和隱私權法規，例如歐盟的《一般資料保護規則》（GDPR）和美國《健康保險可攜與責任法》（HIPAA）。確保第三方 API 的安全性有助於組織遵守這些法規並避免監管機構的處罰。

涉及第三方 API 的安全事故可能會損害公司的聲譽，導致客戶信任的喪失，並可能影響商業夥伴關係。以下是確保第三方 API 安全的 5 項最佳實踐：

一、維護包含第三方 API 清單

維護一個能在程式碼變更時自動更新的 API 清單，會是 API 安全計畫的重要第一步，應用安全狀態管理平台供應商 Bionic 安全研究員 Jacob Garrison 表示。這是 API 安全計畫的重要第一步；它應該區分第一方 API 和第三方 API 的不同。它還鼓勵對地下IT（在未通知安全團隊的情況下就導入的 API）持續進行監控。

「為了確保你的清單強健且可行，你應該追蹤哪些 API 傳送了業務關鍵資訊，例如個人身份資訊和支付卡資料，」他說。API 清單是與第三方廠商風險管理相輔相成的，根據 Garrison 的說法。當開發人員使用第三方 API 時，考慮對供應商本身進行風險評估是值得的。

「例如，假設你的資料工程團隊想要發送個人身份資料到 Tableau 商業智慧分析軟體進行分析，」他說。「在這種情況下，有必要評估該供應商的安全狀況是否在你組織的風險承受範圍內。」

Web 應用安全供應商 Invicti security 技術長暨安全研究負責人 Frank Catucci 也認為，包括第三方 API 的清單將會非常重要。

「你需要讓第三方 API 成為你整體 API 清單的一部分，你必須把它們視為你所擁有且需負責的資產，」他說。「所以，確保你能夠精準計算哪些 API 在哪裡運行以及它們在做什麼，這是重要的第一步，因為你無法保護你不了解的東西。」

二、調查第三方 API 的供應商

根據 McKenney 的說法，組織應該選擇具有強大安全措施且信譽良好的供應商，監控 API 活動

是否有任何可疑行為並使用加密的情形。舉例來說，只使用來自可信賴供應商的支付處理 API，定期監視 API日誌中是否存在任何異常活動，並確保透過 API 發送的所有敏感性資料都是加密的。

利盟（Lexmark）資安長 Bryan Willett 表示，對於第三方廠商來說，建立供應商安全管理流程非常重要。「這個過程應該與你的採購流程緊密結合起來，如此一來所有的供應商和契約都要透過這個流程才行，」他說。「這個流程應該由幾個子流程組成，包括供應商風險評估、供應商安全評分、持續監控以及合同審查，以確保條款符合組織的風險承受能力。」

三、確保供應商進行第三方API安全測試

Willett 說，重要的是，公司需建立供應商的通用安全控制，以及跨第三方 API 生命週期不同階段的安全控制，以確保適當的安全防護能符合他們的風險承受能力。

他進一步指出：「舉例而言，你希望在組織的文化中看到安全開發生命週期從培訓到交付過程中的各個環節都能得到貫徹，以確保從一開始就考慮到安全性。」根據 Willett 的說法，這些環節應該包括解決由供應商所開發原始程式碼和產品中包含的開源程式庫所產生風險的實際做法。

「你希望看到供應商有良好的安全測試實踐，使用最新的工具來執行靜態程式碼分析、模糊測試和漏洞掃描，」Willett 說。「在營運領域，你希望看到強大變更管理流程的證據，對資料進行適當的存取控制，並實施零信任原則。」

供應商還應該有成熟的漏洞管理計畫來監控漏洞修補程式的操作環境，並有一個明確的服務等級協議（SLA）來確定何時修補漏洞。

四、親自測試第三方 API

即使第三方 API 並非由組織所編寫，也非組織所能完全控制，Catucci 說他們仍然可以像測試自己的 API 一樣測試它們。例如，公司可以使用動態應用程式安全測試（Dynamic Application Security Testing，DAST）功能來掃描第三方 API，以尋找已知漏洞和有安全疑慮的元件，抑或可能存在於這些 API 中的過時元件。

「即使你不擁有這些 API，你也必須對它們進行測試，」他說。「如果你發現第三方 API 有特定的安全漏洞，你可能想要禁用該功能，或者在修復之前不再使用該 API。」

五、輪換 API 金鑰

另一個安全考慮是 API 金鑰的輪換，Willett 表示。當使用者呼叫第三方 API 時，他們必須在他們的請求中提供一個稱之為金鑰的獨一無二字串。這個字串告訴供應商哪個客戶正在進行呼叫。定期輪換金鑰通常根據有兩個主要原因。

「首先，惡意攻擊者會攔截你的 API 金鑰，然後他們可以代表你生成請求。根據第三方廠商所使用的安全協定，這個金鑰可能足以提取與你帳號相關的敏感資訊，」Willett 說。「其次，第三方 API 需要花錢。API 金鑰用於計費目的。惡意行為者可以使用你的金鑰快速觸發 API 請求，從而提高你的帳單。基於這兩個原因，API 安全程式應該包括定期的金鑰輪換。」

安全底線：別讓 API 不受保護

基於 API 的攻擊非常複雜，所以需要同樣強大的安全防禦措施。此外，API 安全防護平台供應商 ThreatX 安全策略總監兼資安長 Jeremy Ventura 表示，現在第三方廠商的安全事故比以往任何時候都更加突出。

「許多引人注目的資料外洩安全事故，比如 Peloton 和 Nissan，都是由未受保護的 API 造成的，」他說。「攻擊一個組織的供應鏈對那些想要入侵網路的網路犯罪份子來說非常有吸引力。」

因此，對於企業最重要的是，瞭解第三方 API 安全威脅不僅僅是一個IT 問題，而是一個影響所有組織和客戶的核心業務問題，Ventura 補充道。