radware

Web 應用程式和 API 保護的狀態

執行摘要

世界各地的組織都藉助 Web 應用程式和行動應用程式與客戶、業務夥伴、供應商和員工保持聯繫。應用程式推動著各種工具的運作，從極度複雜的電子商務引擎到雲端式的生產力解決方案，乃至行動電話上的個人工具。

為了加快數位轉型的腳步，各個組織已投注心力於建立和強化應用程式。因此，相較於以往，開發環境和生產環境變得更加靈活且富有彈性，結合許多相互連通的獨立元件，並促進提供安全的應用程式。

而這種複雜性衍生出許多漏洞，導致應用程式的受攻擊面變得無比廣闊。開發人員會仰賴應用程式開發介面 (API) 來連結應用程式，以便共用資料和推動功能。然而，API 往往最容易成為惡意攻擊者入侵目標網路的入口。

為了更加瞭解應用程式和 API 安全性的狀態，Radware 協同 Osterman Research，針對近期的應用程式基礎結構和資料安全性領域開發案例進行了研究。這兩家公司訪問了全球各個行業中的 200 多名中大型企業專業人員。

這份報告驗證了組織的應用程式在認知、可見度、實務和策略方面的安全性程度，還揭示了不同的使用案例和商業效益、審視不同角色如何看待應用程式的安全性，並探索安全性決策對於業務成果的影響。API 安全性是這份報告中特別關注的重點，目的是為了瞭解在不同的應用程式開發和生產環境下，業務目標和安全性風險的對照情形。

應用程式開發和傳遞的狀態

- 98% 的受訪者回報，其應用程式在 2020 年曾受攻擊。
- 70% 的生產應用程式位於私有雲端或由公用雲端提供者代管，而非公司的資料中心內。但是，開發中的應用程式不太可能託管給公用雲端。
- 57% 的組織已經使用容器化的應用程式，然而，有 52% 的受訪者認為，使用容器並未帶來任何財務效率。
- 大多數資歷較深的受訪者確信，新的技術能提供相同水準以上的應用程式安全性，但在受訪者當中，對此的信心會隨著是否擔任負責安全性的職位而有所不同。
- 在 92% 的組織中，安全性員工對於持續整合/持續部署 (CI/CD) 架構沒有發言權，並且在大多數情況下都必須維持現狀。在 89% 的組織中，資訊安全性小組沒有安全性解決方案的預算。

威脅態勢

API 是下一個重大威脅

- 容易建置和容易取用的 API 在加快應用程式開發速度的同時，也會在系統之間傳遞敏感資料。將近五分之二的組織有超過一半的應用程式透過 API 向網際網路或第三方服務公開。
- 組織日益關注 API 安全性領域。55% 的組織指稱這是「當務之急」，而 59% 的組織則表示，打算在 2021 年「大幅投資」此領域。

企業還沒做好正確管理 Bot 流量的準備

- 82% 的組織表示受到 Bot 攻擊困擾。
- 雖然市面上有專門的解決方案能夠偵測和對抗不合法的 Bot 活動，但只有四分之一的組織採用。受訪者表示，Bot 攻擊比其他類型的攻擊更有可能成功，然而只有 39% 的受訪組織有信心應付複雜的惡意 Bot。

阻斷服務 (DoS) 攻擊仍非常普遍，而且大多數量龐大，甚至還會針對應用程式

- 以網路層級的攻擊來說，DDoS 是最常用來攻擊應用程式的媒介。89% 的受訪者表示遭遇過這類針對 Web 應用程式的攻擊，三分之一的受訪者每週都受到攻擊。應用程式層的 DDoS 攻擊通常採用 HTTP/S 洪水的形式。
- 80% 的受訪者表示應用程式受到 DoS 攻擊。

98%
的受訪者回報，其應用程式在 2020 年有受到攻擊。

70%
的生產應用程式位於於私有雲端或託管給公用雲端提供者

57%
的組織已經使用容器化的應用程式

92%
的組織中，安全性員工對於持續整合/持續部署 (CI/CD) 架構沒有發言權

行動應用程式非常不安全

行動應用程式在 2020 年扮演了重要角色，因為大多數的資訊工作者在這一年都轉為在家工作，因此要仰賴行動應用程式來進行工作、教育、娛樂、社交互動和其他活動。不過，行動應用程式的開發非常不安全。

- 大部分的組織並未在行動應用程式上套用與 Web 應用程式同等的安全性措施。只有 36% 的行動應用程式已在行動應用程式的開發生命週期完全整合安全性，而有一大部分的組織不是完全沒有安全性 (22%)，就是只有「附帶的」安全性 (42%)。而行動應用程式經常是由第三方開發，因此擁有敏感資料的企業應該留意安全的開發做法。

移轉至公用雲端會引發信任問題

- 只有 27% 的組織「完全信任」雲端提供者所提供的安全性。
- 在已移轉至公用雲端的組織之中，有 47% 使用不只一個基礎結構提供者來託管其生產應用程式。
- 移轉至公用雲端往往會導致對於應用程式安全性的誤會和信任問題。調查發現，隨著組織使用公用雲端的比例上升，對於公用雲端會施加強大安全性的信心程度卻下滑。
- 37% 的組織未察覺可能已經發生的資料洩漏情形。

近期的應用程式安全性

- 最常見的應用程式安全性管理疑慮是跨平台原則一致性和事件的可視性。
- API 濫用將是首要威脅，並且也是近期的投資重點。
- 55% 的組織表示，應用程式和 API 的安全性將是 2021 一整年的高度優先或極高度優先事項。
- 59% 的受訪者表示，將會在 2021 年投資或大幅投資 API 保護，以解決其一致性和可視性方面的疑慮。

大部分的組織並未在行動應用程式上套用與 Web 應用程式同等的安全性措施。

36% 只有 36% 的行動應用程式已在開發流程中完全整合安全性

下載免費報告

radware