2022 年我們不能忽視的網路安全問題

翻譯及整理｜叡揚資訊 資安事業處

> COVID-19 改變了我們過去生活及工作的方式，過去兩年對我們的網路安全系統來說是一場烈火的洗禮。企業採用了遠端工作模式，網路安全藍圖因而受到了考驗。做為一個企業，我們真的必須提高警惕和適應，特別是網路攻擊事件大流行，駭客攻擊事件比例，已超過往年 300%。

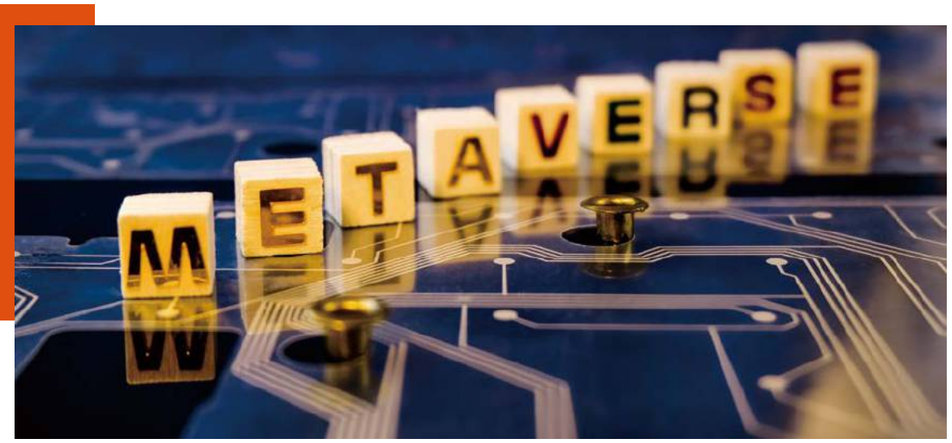
有鑑於此，網路安全的議題更加被重視，安全的應用系統和程式碼也相對更顯重要。美國總統拜登先生，頒佈關於軟體供應鏈安全的行政命令裡，特別闡明了關鍵問題，尤其是在 SolarWinds 大規模漏洞事件之後。我們都需要更加地關心安全問題，並努力透過多種安全檢測工具，以減少漏洞的發生，造成更嚴重的資安事件危害。也就是說，與網路駭客交手過程中，我們需要盡可能地與他們保持同步，且以預防的心態搶占他們攻擊的場域。

元宇宙是另一個攻擊對象

元宇宙可能是網際網路的下一個發展目標，但大多數企業對於如何建構安全的應用系統及數位化環境，還沒有更具體的轉變及想法。

雖然像網路釣魚詐騙這樣的安全攻擊事件頻傳，但虛擬世界的盛行，以及沉浸式 (immersive) 的社群工具發展，仍需兼具考量基礎設施及設備之安全性。智慧型手機的時代幫助並豐富我們現在的生活方式，像 VR 耳機新穎的週邊電子設備，其用戶會有大量數據存取，亦為資安開啟了新的大門。

越來越複雜的嵌入式系統安全，需要確保物聯網工具的安全性，主流 VR/AR 的應用也不例外。正如我們在 Log4Shell 漏洞內容中看到的一樣，簡單的程式碼錯誤，可能成為駭客取得登入後台的通行證，而在虛擬世界中，每一個動作都會產生可能被竊取的數據風險。



雖然處於起步階段，但一個成功的元宇宙將需要實際採用加密貨幣（而不是隨意囤積最新的紀念幣）以及像 NFT 等有價值的項目，這意味著我們現實生活中的財富、身份、數據和生計來源，可能開拓出一個需要關注新的資安領域，而使我們陷於危險之中。在我們工程師開始瘋狂地開發像史詩般的功能和強化功能之前，你可以優先選擇，將這個新創的、巨大的攻擊面最小化。

Log4shell 事件後的規範建立

Log4Shell 事件發生後，大家陷入混亂、疲於奔命地尋找是否存在任何具相關性之實例或廣泛被使用的 Log4j 日誌工具版本，這對程式開發人員無疑是一件不願樂見的事。這種零時差攻擊，是有史以來最糟糕的攻擊之一，人們將 Log4Shell 與毀滅性的 OpenSSL Heartbleed 漏洞相提並論，即使超過六年這類型的漏洞仍然存在著。

由此看來，我們在未來很長一段時間內需處理 Log4Shell 所帶來的問題。即使從 Heartbleed 事件中獲得了教訓，我們需要盡快推出修補漏洞的程式，但許多企業仍然沒有足夠快的行動來保護自己。比較大的公司，修補漏洞可能非常困難或具官僚主義，需要跨部門的文件與程序，很多時候 IT 部門與開發人員對所有正在使用的函式庫、元件、工具沒有全面性的了解，而開發時又有嚴格的部署時間表，所以會盡可能減少中斷和應用系統的停機時間。這種工作方法有其合理的理由，因為沒人想打亂了開發計畫，但修補漏洞太慢就是坐以待斃。

正如 SolarWinds 攻擊改變了軟體供應鏈的遊戲規則一樣，我們預測在 Log4Shell 之後也會發生類似的情況。雖然在一些關鍵產業中，已經有修補管理的授權和建議，但廣泛性的規範建立是另一回事。預防性的軟體安全永遠是我們完全避免緊急修補漏洞最好的機會，但最好的作法還是有漏洞時馬上修復。

重視架構安全（但開發人員沒準備好）

由新的 OWASP Top 10 2021 中可看到，其新增的漏洞類型與新的排列方式，Injection 漏洞從第一名跌至第三名。這些新增的漏洞類型說明開發人員在撰寫安全程式碼及識別漏洞、修補漏洞等階段，除非經過適當的培訓，否則大多數的開發人員是沒有能力降低風險的產生。

我們已經知道，如果我們要對抗程式碼中常見的安全漏洞，開發人員必須具備安全知識的技能，而企業對於培訓開發人員良好的資訊安全能力，是需一套長期且有效的培訓計畫。

不安全的程式設計 (Insecure Design) 在 OWASP Top 10 中佔有一席之地，它不止是單一類型的安全漏洞，而是整體程式安全架構的風險問題，對於開發人員來說，不止是了解其中某一個漏洞類型而已，還需要掌握整體 Insecure Design 相關安全漏洞。全面性漏洞學習環境，最好在安全團隊的支持下進行，且在開發人員成功提升資安能力後，可減輕團隊內的壓力，但就目前實際況狀而言，對大多數軟體工程師來說還未建立這樣的安全程式培訓觀念。

對抗這樣的情況，從西方的一個諺語「It takes a village」可了解，企業應該為團隊開發人員提供良好的資訊安全培訓平台，在不影響開發人員開發進度下，積極的將資訊安全培育的觀念導入企業中，讓資訊安全議題融入企業文化中。