社交工程攻擊防範及建議

關於台灣二版

Version 2 是代表再進化的意念。藉由不斷成長、蛻變且與時俱進。

在西方象徵勝利，而雙數在東方蘊含著吉祥；集聚東西方思維，彈性不僵化。

台灣二版 (Version 2)是亞洲其中一間最有活力的 IT 公司，多年來深耕資訊科技領域，致力於提供與時俱進的資安解決方案 (如EDR、NDR、漏洞管理)，工具型產品 (如遠端控制、網頁過濾) 及資安威脅偵測應變服務(MDR) 等，透過龐大銷售點、經銷商及合作伙伴，提供廣被市場讚賞的產品及客製化、在地化的專業服務。

台灣二版(Version 2) 的銷售範圍包括香港、中國、台灣、新加坡、澳門等地區，客戶涵蓋各產業，包括全球1000大跨國企業、上市公司、公用機構、政府部門、無數成功的中小企業及來自亞洲各城市的消費市場客戶。

何謂社交工程?

- 什麼是社交工程？做什麼用的？
  - 社交工程是一種利用人心的資安攻擊手法，主要目的為：
    - 竊取資料
    - 獲取利益
    - 入侵設備
    - 冒用身分
  - 任何人都可能被假冒或成為受害者。
  - 利用各種方式取得目標資訊，透過寄送電子郵件、 路邊的USB、假網站方式對目標進行攻擊。

社交工程定義	駭客利用各種方式取得目標資訊。
攻擊危機	就算有再好的資安設備，高效能防護系統，只要有**人為操作**，就有遭受社交工程的危機。
攻擊目的	系統破壞、網路癱瘓，惡意廣告、植入惡意程式、挖礦、盜取個資流入黑市、金錢等目的
社交工程造成極大威脅的原因	利用使用者對於資訊詐騙沒有足夠認知來騙取個資等機敏資訊，不需要專業技術的犯罪行為

常見的攻擊手法

- 利用電話佯裝資訊人員，騙取電腦設備的帳號密碼。
- 偽裝委外廠商需要連線，騙取電腦設備的帳號密碼。
- 網路釣魚：騙取用戶點擊連結或下載。
- 利用郵件誘騙開啟圖檔或者利用工具誘騙下載，植入惡意程式後暗中收集機密資料。
- 利用即時通訊系統誘騙點選連結後，導致電腦設備中毒。


偽裝委外廠商
帳號及密碼
網路釣魚
利用郵件誘騙開啟圖檔
植入惡意程式
暗中收集機密資料
利用工具誘騙下載(如P2P)
植入惡意程式
暗中收集機密資料
利用電話
佯裝資訊人員
騙取帳密
利用即時通訊軟體
誘騙點選連結後中毒

社交工程攻擊對企業的影響

社交工程攻擊本身只是駭客突破企業網路的一個手段，其真正的危險在於造成資訊安全的破口，從而降低工作效率，造成企業經濟損失。常見的情況有：

- 郵件變臉詐騙。
- 勒索病毒造成資料損失及癱瘓系統、產線停擺。
- 機敏資料外泄。
- 挖礦病毒挖走設備資源。
- 僵屍網路，攻擊打手。

社交工程防範

社交工程防範

- 基本防範
  - 執行各種作業系統、應用軟體更新及設定
  - 要安裝防毒軟體，並定期更新
  - 密碼設定強度及複雜度要足夠，使用不重覆的密碼，不同系統間使用不同密碼
- 網路釣魚防範
  - 點選連結前，先移動滑鼠檢查來源
  - 收到要求提供個人資料的電子郵件要小心
  - 小心威脅要錢的電子郵件或其他訊息

漏洞管理

組織可以透過識別、分析判斷和處理潛在**安全性弱點**來**防範**攻擊，並在發生威脅時盡量降低損害

漏洞管理的目標是透過盡可能**緩解弱點**，藉以降低組織的整體曝露風險

弱點管理應是**持續性的程序**，需要跟上新的威脅和不斷變化的環境

vRX

漏洞管理解決方案

- TOPIA 為企業提供保護使用的作業系統與第三方軟體避免受漏洞的影響。
- 威脅分析工具針對作業系統與第三方軟體進行二進制分析，識別高風險漏洞，包括0-DAY和CVE 。

VRX

分析

- 應用程式自動識別
- 應用程式威脅分析
- 資產威脅分析

優先

- **xTags**
- 應用程式與資產風險評估
- 優先級別圖表

行為

- 推薦操作引擎
- 實時修補程式管理
- 無修補程式保護

網頁過濾

網頁過濾是一種透過阻止使用者的瀏覽器載入某些網址或網站的頁面來阻止使用者查看這些網站的技術。網路過濾器以不同的方式製造，並為個人、家庭、機構或企業使用提供各種解決方案。

一般來說，網頁過濾器以兩種不同的方式運作。他們可以透過查閱已知清單來阻止根據網站品質確定的內容，這些清單對所有內容類型的流行頁面進行記錄和分類。或者，他們可以即時評估頁面內容並相應地阻止它。許多網頁過濾工具都基於不斷更新的網址資料庫，該資料庫顯示哪些網站和網域與託管惡意軟體、網路釣魚、病毒或其他有害活動工具相關。

SAFEDNS

網路過濾解決方案

- SAFEDNS為企業提供安全的DNS解析服務。
- 針對惡意軟件、殭屍網絡、勒索軟件和網路釣魚透過DNS的保護，可使企業或使用者減少被駭客與病毒攻擊的機會。

SAFEDNS

- 人工智慧過濾技術
- 過濾質量監控
- 類別過濾
- 過濾定制
- 高準確率

安全的加密網路

公共網路可能不受防護，例如某個 Wi-Fi 網路使用不安全的加密協定或薄弱密碼。當您透過不安全的 Wi-Fi 網路傳輸時，您的密碼或其他機密資訊將以非加密資料傳輸。駭客可以攔截您的機密資料，找出您的金融卡密碼或操作您的帳戶。

由於新冠病毒大流行，傳統工作空間的型態有了翻天覆地的變化。遠距工作已成為一種主導趨勢。

遠端安全存取解決方案

- NordLayer是一個完全無需硬體的安全網路存取解決方案，您可以在幾分鐘內開始使用它。NordLayer遠端存取解決方案是專為企業而設計的，能夠幫助企業減少風險、當遠程工作時保護公司免受網路威脅。

NORDLAYER

- 2FA
- 單一登入
- 生物辨識認證
- 網路分段
- SITE TO SITE
- AES 256加密
- 威脅攔截
- 使用者配置
- DNS過濾
- 虛擬專用GATEWAY
- 活動資訊

無密碼時代的來臨

在如今的網路世代，人人都有許多線上帳號。而隨著帳號盜用事件的層出不窮，各界也開始對資安日趨重視，就在網路日漸發達、雲端軟體服務四起以及科技日新月異的背景之下，造就了新世代的網路識別標準 FIDO（Fast Identity Online）的問世。

由於Q-Day即將到來，傳統以帳號密碼驗證身份的方式已不再是科技巨擘們眼裡最安全可靠的登入途徑了。

NordPass

密碼管理解決方案

- NordPass是一款安全、簡單且功能強大的密碼管理器。NordPass提供雙因素認證，提升使用者的安全等級。使用NordPass可以輕鬆生成強密碼、安全地共享密碼，並檢查您的資料是否曾遭遇過洩漏。

NORDPASS

- 密碼儲存管理
- 自動填寫
- 生成強密碼
- 數據安全
- 跨平台同步
- 安全共享
- 密碼健康檢查