網路開店資安防護介紹

財團法人資訊工業策進會 資安所

林耕宇 正工程師

資料外洩主要管道說明

- 伺服器端遭駭客入侵將資料外洩

  任何對外之伺服器均有可能遭駭客入侵，目標可能是應用程式、掛載之服務或作業系統之漏洞遭利用或設定疏忽所造成

  1. 作業系統沒有更新
  2. 應用系統突然換人維護
  3. 外掛的服務被找到漏洞

- 擁有權限之使用者端電腦遭惡意程式感染或駭客入侵

  1.登入後台期程過久

  2.下載訂單資料但是沒有再次驗證下載的身分

- 擁有權限可存取敏感性資料之使用者端電腦遭感染或駭客入侵，導致敏感性資料遭外洩

  已經出貨的訂單資料持續留存，未刪除

供應商的基本資訊安全觀念

- 使用正版軟體，防毒軟體，定期更新
- 使用至少15位元英數字的密碼，長度比複雜度更重要
- 盡可能使用固定IP 連線到後台，如果沒有固定IP 也應該使用手機驗證碼二次認證

供應商面對的問題

- 發生資安問題， 不敢面對現實
- 至少要求平台應證明資安做的夠好， 例如定期更新的紀錄，弱點掃描的報告，架構足以抵擋暴力的攻擊

平台商資安管理需注意之問題

- 檢視所有對外主機
  - 是否有對外伺服器疏忽？(電話通信主機/CCTV/測試機...)
  - 是否正常執行更新， 弱點掃描
  - 帳密管理
  - 遠端存取管理(後台管理)
  - Log 稽核
- 委外管理
- 異常能否查覺

平台商必須面對的問題

- 普遍認為後台系統提供供應商自行管理帳號與密碼，但不負保管的責任。
  1. 管理供應商必須守法使用正版軟體，防毒軟體
  2. 規範用戶登入不只帳號與密碼
  3. 管理連線時程
  4. 下載訂單時必須二次驗證確認身分

駭客入侵之主要管道

- 人為的疏失造成
  - 設定或管理疏失
  - 下載及執行被偽裝的程式或檔案
- 駭客入侵
  - 大多利用系統或應用漏洞
    - 作業系統漏洞 / 服務漏洞(FTP、Http 、 DNS 、 Mail / 網站漏洞 / 應用軟體漏洞...等路徑)
  - 若漏洞被駭客發現早於系統修補時間
    - 零時差攻擊

使用政府提供的資源

EC Cert+ 是網購業者之資安小幫手

提升網購交易資安環境、深化網路交易資安管理

資安服務

協助網購業者：
- 資安應變諮詢
- 資安技術協處
- 提供資安改善方案
- 查驗資安檢測報告

資安推廣

- 網路零售業資安基本查核表
- 網路零售業個資防護廠商自評表
- 網購零售資安管理參考手冊
- 促進網路零售業者與資安專家經驗交流

資安輔導

協助主管機關(商業司)：
- 推動資安基本要求
- 擔任資安技術幕僚
- 安排實地資安訪視
- 籌辦個資行政檢查

資安聯防

- 資安事件通報
- 資安情資交換
- 資安警訊發布

網路零售業個資與資安管理參考手冊

藉由資安訪視以及個資行政檢查相關案例發現，掌握對業者實施資安 / 個資管理有助益之主題，編撰網際網路零售業個資與資安管理參考手冊。

主題如下：

個資保護	資安防護
電商網站隱私設計	防毒軟體重要性
委外資服業者	後台疑點
事故通知	系統弱點防護
個資跨境傳輸	管理階層心態

感謝聆聽　敬請指教

服務網站：ec-cert.org.tw
服務專線：6607-3284
服務信箱：service@ec-cert.org.tw