|  |  |
| --- | --- |
| **預防網站個資外洩參考說明** | |
| 一、必須先瞭解網站架構與弱點所在（如資料隱碼攻擊、跨站腳本攻擊、惡意程式或人為因素等） | 每個網站與資料庫型態不同，應協同所屬公司進行內部分析，並透過整體檢視與共同討論找出問題，並可參照國外OWASP組織所揭露常見的網站應用程式十大弱點，清查網頁應用程式與網頁服務安全性：   1. 跨站腳本攻擊(Cross Site Scripting，簡稱XSS)。 2. 注入漏洞攻擊(Injection Flaw)。 3. 惡意檔案執行(Malicious File Execution)。 4. 不安全的物件參考(Insecure Direct Object Reference)。 5. 跨網站的偽造要求 (Cross-Site Request Forgery，簡稱CSRF)。 6. 資訊揭露與不適當錯誤處置 (Information Leakage and Improper Error Handling)。 7. 遭破壞的鑑別與連線管理(Broken Authentication and Session Management)。 8. 不安全的密碼儲存器 (Insecure Cryptographic Storage)。 9. 不安全的通訊(Insecure Communication)。 10. 疏於限制URL存取(Failure to Restrict URL Access)。 |
| 二、研判駭客入侵方式與手法（內部發動或外部進入） | 1. 週末或連假為駭客入侵高峰期，若公司內部無人看管網站資訊，發生資安事件亦無法即時反應。建議非上班時段，公司內部系統應強化偵測木馬程式及異常存取行為，並能調度專人適時因應。 2. 公司內部所含資訊部門人員，應具備瞭解駭客所用常見語法、系統入侵前後異狀-有無惡意程式、進入方式、個資竊取方法、接收個資方式等相關能力。 3. 公司資安系統應具備稽核駭客進入資料庫IP來源，或者攻擊前的惡意掃瞄或測試行為（日誌記錄檔常可見多筆錯誤訊息）。 4. 其他：類似網站犯罪手法或可以歸納犯罪者相關特徵（例如入侵後可能會新增哪些檔案或圖片，可能與竊取個資無關，駭客可能用來證明特定身份之用途等）。 |
| 三、採用防制手段（異常客戶狀況、焦點討論、清查LOG、修補漏洞或重置） | 1. **異常客戶狀況**：   駭客為熟悉網站狀態，常於發動攻擊前會申請網站會員或使用相關服務，可能留下相關線索。   1. **焦點討論**：   公司網管人員應先研究如何調查出異常對象，如果無法找出問題，必須先盡可能阻斷所有個資外洩管道。   1. **清查LOG**：   網站相關LOG檔案，必要時請提供光碟片予轄區警方(偵查隊或刑警大隊科偵組等)進一步追查。   1. **修補漏洞或重置**：   落實權限控管，包括監控特權系統帳號的存取行為、強制存取路徑、定期安裝管理修正程式等控制措施，並安裝Client或Gateway端的防毒軟體，降低電腦被植入木馬程式的風險 |
| 四、補救措施（主動式犯罪預防宣導、配合後續入侵追查） | 1. 透過近期犯罪手法分析，犯罪者會在週末假日進行個資竊取與詐騙活動，請務必留意公司網站資料庫，假日是否派員留守維護等，另客服系統也可以對於民眾接獲詐騙電話後提供即時諮詢，有效防堵。 2. 個資外洩後宣導民眾仍為重要工作，駭客把個人資料交給詐騙集團，透過境外發話（**國內顯示來電都會出現＋開頭電話，例如＋02 或＋0800**）進行詐騙，主要還是以分期付款設定錯誤，誘騙民眾到ATM匯款，所以請業者務必做好緊急應變狀況（例如：主動簡訊發送宣導）。 3. 後續觀察犯罪後結果成為重要關鍵指標，除可瞭解業者防堵後有無效度，透過與轄區警方定期聯繫瞭解最新犯罪動態，以整合有效防治力量。 |
| 備註 | 本說明表為彙整國內常見網站個資外洩之相關防制措施，供電子商務業者自行審視稽核參考。 |