網路零售業
如何提高組織的資安防護
參考指引

政策行動

1. 建立並確認資安政策與組織人員之資安職責，落實執行整體資安政策。
2. 鑑別和盤點記錄組織基本資訊文件（紙本與電子）並定期備份。
3. 規範密碼政策並落實執行。
4. 決定組織人員與客戶需要什麼樣資訊的存取權限，依據工作角色需要控制他們可存取系統和資訊。
5. 確定哪些員工需要存取USB權限，並確定USB實體擁有管理者。
6. 管理並定期審查USB權限清單，並清查USB實體擁有者之管理作為。
7. 業務委外服務事項，應確認於委外服務合約內容應包含個資保護與資安防護要求事項。
8. 訂閱資安威脅與弱點警報並閱讀相關應對建議並與組織人員分享。
9. 確保組織人員獲得資安所需的知識和技能。
10. 將資安措施作為正式的內部規範並落實執行資安要求事項。

技術行動

1. 應由技術人員來負責執行設備、網路與軟體的設置和配置。
2. 使用防火牆防護工具，保護網際網路。
3. 安裝並啟用防毒軟體，安排定期手動檢查更新。
4. 關閉不使用的通訊埠。
5. 執行密碼管理政策並強制使用，對所有敏感資料之帳號，啟用雙因子驗證機制。
6. 確保資料備份成功。
7. 限制並防止人員或系統下載第三方應用程式。
8. 在所有設備上安裝最新的軟體更新並定期開啟自動更新檢查，安排定期手動檢查更新。
9. 考慮在所有辦公設備上設置加密措施。
10. 全面執行弱點掃瞄並定期執行檢查、修補漏洞。

培訓和意識行動

1. 應確定執行實施員工資安防護培訓和意識宣導訓練。
2. 團隊的每一位成員（包括董事會成員）需要充分的了解資安的知識與資安對組織的影響。
3. 提供安全的實體存儲設施（例如上鎖的櫥櫃）供員工文件記錄和存儲電子檔案媒體。
4. 建立並實施資訊安全培訓計畫，並應納入全體員工。
5. 密碼政策應詳細說明，並教授如何創建安全的密碼與使用方法。
6. 實施電子郵件與網際網路之安全使用方式。
7. 教導如何發現網絡釣魚的明顯跡象。
8. 建立並實施資訊安全事件通報與應變及報告等過程的詳細作業要求。
9. 提供安全的業務運作服務方式和如何利用電子郵件處理內外部服務請求。
10. 提供Wi-Fi熱點漏洞的詳細資訊以及如何使用替代方案選項（例如VPN／行動網路）。