網絡安全七大攻略

1. 保安政策和安全管理

- 訂定並記錄與網絡安全風險有關的保安規定
- 定期覆檢和更新保安規定和保安政策
- 定期向員工傳閱有關最新保安政策的資訊

2. 端點保安

- 安裝防病毒和抗惡意程式碼軟件等保安軟件
- 保持保安軟件的病毒定義檔和修補程式為最新版本
- 保持端點的作業系統及軟件為最新版本
- 在日常使用時，應使用非特權及非管理員帳戶登入

3. 網絡安全

- 配置防火牆以保護機構的網絡，並減少連接至互聯網上的網絡端口
- 防火牆上的默認規則應為「DENY」（拒絕）根據業務需求，僅允許網絡流量
- 僅允許已轄准的 IP 地址連接至互聯網
- 使用安全的VPN連線進行遠端存取
- 使用加密的網絡傳輸規約（如HTTPS）
- 定期覆檢防火牆規則

4. 系統安全

- 啟用安全策略並關掉無需使用的服務以強化系統安全
- 保持系統所有軟件（包括作業系統、保安軟件、修補程式等）為最新版本
- 將儲存在系統的敏感資料加密
- 應用程式應驗證和過濾來自互聯網使用者的輸入（如網站表格），以避免如SQL注入類型的攻擊
- 定期進行保安風險評估及審計

5. 保安監控

- 啟用網絡設備（如防火牆）和伺服器記錄功能
- 集中儲存記錄，以便進行定期審查和監控
- 審查記錄和保安警報，並對找出問題地方及時作出應變
- 監控網絡流量（如互聯網流量），以檢測流量模式是否有異常

6. 事故處理

- 為處理不同種類的保安事故（如勒索軟件、數據外泄、分散式拒絕服務攻擊等）制定事故應變計劃
- 定期備份系統和數據
- 保持備份離線（異地儲存更為理想）
- 定期進行備份復原演習，以確認數據能夠穩妥地復原

7. 用戶意識

- 透過員工意識培訓等定期提醒員工在保護機構的訊息資產方面的角色和責任
- 進行演習（例如模擬仿冒詐騙攻擊），以測試員工應對常見網絡攻擊的準備情況

GovCERT.HK 政府電腦保安事故協調中心
HKCERT 香港電腦保安事故協調中心
香港警務處 Hong Kong Police Force

詳情請瀏覽「香港電腦保安事故協調中心網站」：
www.hkcert.org