資安事件處理建議措施

這份資安事件處理建議措施提供了一些基本的防護與檢測方法，例如安裝防毒軟體、修補系統漏洞、啟用防火牆、檢視異常帳號與連線等，希望可以幫助使用者更全面地應對資安事件。

1. **防毒與惡意程式掃描**
   - Linux：使用 ClamAV 進行掃描。
   - Windows：使用 MS Windows 內建的 Microsoft Defender、學校提供的校園版防毒軟體或 Malwarebytes 進行全機掃描，並確保病毒碼持續更新。
2. **系統漏洞修補**
   - Linux：使用 apt update && apt upgrade 或 yum update 來更新系統。
   - Windows：使用 Windows Update 來確保系統與應用程式的安全性更新已安裝。
3. **防火牆與網路連線管理**
   - Linux：使用 iptables 或 ufw 來管理網路流量。
   - Windows：使用 Windows Defender Firewall 或是校園版網路防護軟體提供的防火牆功能，設定入站(輸入)與出站(輸出)規則。
   - 對於靜態網站，建議除系統更新或資料同步需求須對外連線的埠(port)外，其餘對外連線全面封鎖。
4. **異常帳號與登入檢視**
   - Linux：使用 cat /etc/passwd 檢查帳號、last 檢視登入紀錄。
   - Windows：使用 Local Users and Groups (lusrmgr.msc) 檢查帳號，使用 Event Viewer (eventvwr.msc) 檢視登入紀錄 (Windows Logs > Security、查找 Event ID 4624)。
   - 查找重點：系統帳號重名、無人使用帳號、某段時間應該沒人登入，卻有登入紀錄？
5. **異常連線檢查**
   - Linux：使用 netstat -tunlp 或 ss -tulnp 來檢查異常連線。
   - Windows：使用 netstat -ano 或 TCPView (Sysinternals 工具) 來檢視開啟的連線與對應的程序。
6. **異常程式檢視**
   - Linux：使用 ps -Af 檢查執行中的程序、crontab -l 檢查排程任務。
   - Windows：使用 Task Manager (taskmgr) 檢視執行中的程序，使用 Autoruns (Sysinternals 工具) 檢查開機啟動項目。
7. **備份與系統重灌**
   - Linux：使用 rsync 或 tar 來備份重要資料。
   - Windows：使用windows 系統內建的檔案歷程紀錄(File History)或備份與還原(Backup and Restore)等應用程式來備份重要檔案，必要時使用復原(Windows System Recovery)功能進行系統重灌。

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/faq:incident_response_process

Last update: **2025/06/17 08:31**