出國報告（出國類別：視察）

參與108年度「外交部駐外館處資安防護強化計畫」(資安健診)紐澳線出國報告

服務機關：國家通訊傳播委員會
財團法人電信技術中心
姓名職稱：吳銘仁簡任技正
曾昭銘工程師
派赴國家：紐西蘭、澳大利亞
出國期間：108 年 11 月 07 日至 11 月 22 日
報告日期：109 年 1 月 20 日

摘要

本計畫之駐紐澳外館處資安健診作業，係自 108 年 11 月 7 日至 11 月 22 日於紐西蘭之奧克蘭、威靈頓，及澳大利亞之墨爾本、培拉、雪梨與布里斯本等六個館處，依序進行各駐外館處資通訊設備之資安健診。此行主要目的係經由國內相關資安專業單位組成之資安團隊，以第三方參與方式，協助外交部針對外館資通訊網路及設備進行資安健診作業，以評估及確保各外館處資通訊設備、網路架構、網路品質等皆達一定的資安防護水準。

本會(NCC)及電信技術中心(TTC)負責檢視各館處是否存在異常無線訊號、網路架構及網路品質是否合理，及電信資費評估等事項，以強化外交部的外館單位資安防禦體質，降低資安風險。資安團隊並透過專用資安檢測工具及團隊分工合作，將發現到的惡意活動進行分析追蹤，協助外館單位找出資安問題並且提供改善建議，並且對外館人員進行資安教育宣導，以強化人員的資安防護概念，提升外館單位同仁對於資安防護的重視。

目錄

壹、 目的

協助外交部辦理 108 年度「外交部駐外館處資安防護強化計畫」(資安健診)之紐澳線(奧克蘭、威靈頓、墨爾本、坎培拉、雪梨及布里斯本等)駐外館處資安健診作業，以提升我國駐外代表處的資安防護能力，降低資安風險。本次組團執行資安健診工作的發現部分事項依規定應屬外交部機密，故報告內容主要以作業流程面進行說明。

貳、 行程

日期	預定行程/作業館處
11 月 07 日(四) 至 11 月 08 日(五)	出發 TPE 臺灣桃園國際機場 抵達 AKL 奧克蘭國際機場
11 月 09 日(六) 至 11 月 10 日(日)	**駐奧克蘭代表處資安健診共 1.5 日**
11 月 10 日(日)	出發 AKL 奧克蘭國際機場 抵達 WLG 威靈頓國際機場
11 月 11 日(一) 至 11 月 12 日(二)	**駐威靈頓代表處資安健診共 1.5 日**
11 月 12 日(二)	出發 WLG 威靈頓國際機場 抵達 MEL 墨爾本際機場
11 月 13 日(三) 至	**駐墨爾本代表處資安健診共 1.5 日**

日期	預定行程/作業館處
11 月 14 日(四)	
11 月 14 日(四)	出發 MEL 墨爾本際機場 抵達 CBR 坎培拉國際機場
11 月 15 日(五) 至 11 月 17 日(日)	**駐坎培拉代表處資安健診共 2.5 日**
11 月 17 日(日)	出發 CBR 坎培拉國際機場 抵達 SYD 雪梨國際機場
11 月 18 日(一) 至 11 月 19 日(二)	**駐雪梨代表處資安健診共 1.5 日**
11 月 19 日(二)	出發 SYD 雪梨國際機場 抵達 BNE 布里斯本國際機場
11 月 20 日(三) 至 11 月 21 日(四)	**駐布里斯本代表處資安健診共 1.5 日**
11 月 21 日(四) 至 11 月 22 日(五)	出發 BNE 布里斯本國際機場 抵達 TPE 臺灣桃園國際機場

參、 過程及內容

一、 行前作業

（一） 召開行前會議

健診團隊應召開行前會議，向全體團員說明駐外館處資安概況、配合廠商事前蒐集之情資、健診重點單位、團員工作分配內容及本次健診使用之檢測工具。

二、 健診作業

（一） 健診啟始會議

健診團隊到達每一外館處後，應先與館處共同召開健診啟始會議，向館處全體人員說明健診團隊來意、介紹成員與健診作業內容，同時進行資安教育宣導課程，並由館處主管下達配合健診指示，以提升館處人員合作態度，期能順利執行健診作業。

（二） 健診工具設定與執行健診

健診團隊開始執行健診前，為避免健診工具設定失敗，會先選定一部館處可連網電腦執行健診作業，並確認健診工具與健診資訊蒐集、分析設備間之訊息傳遞正常後，團員才開始執行健診，以降低對館處人員工作之干擾。團員執行健診時，應由外館聯絡人、資安承辦人員帶領進入館處各單位。

在資安健診過程中團員會特別針對廠商事前提供的館處資安情資深入調查，以確認該情資之實際情形，若發現館處資訊設備確實存有高度風險程式或惡意行為，則會將該主機磁碟進行複本作業及深入調查。

本次專案執行過程中，依照團隊分工作業流程，由 NCC 與 TTC 團員針對館處的無線網路、電信網路架構及連線速率進行檢測，並一併評估各館處上網連線資費的合理性，必要時，請配合廠商出席代表提供相關資訊協助。相關作業程序說明如下：

1. 針對駐外館處提供專屬之無線網路進行訊號強度檢測，作為該館處優化通訊參考。
2. 針對駐外館處辦公空間的異波訊號進行掃描，檢測是否存有異常的無線網路訊號，包含可能的無線印表機 WIFI DIRECT 功能是否關閉，以及是否有人員私設無線基地台等情形。
3. 針對館處電信機房及網路架構進行盤點，檢查是否存有國安疑慮的電信設備、存有非單一出入口或異常電路串接等，以確認是否有違反相關資安政策。
4. 在連線速率方面，檢測館處實際對外上網連線速率及品質，包括連線當地電信事業提供的網速測試網頁及連線國內測速網頁，以評估網路架構及網路品質。
5. 在連線資費合理性方面，則評估駐外館處申設寬頻上網服務之資費選項，提供合理性評估及建議。

（三） 健診完成後置作業

健診作業實施時，團員須於館處各連網電腦執行健診工具程式，因程式執行檢測需一段時間而無法即時移除，團員於健診完後會協助移除健診工具程式。

（四） 分析結果相關作業

（一）分析駭侵情資及研擬建議作為

健診作業實施後，若發現有電腦主機存在駭侵情資，健診團隊應整合團隊力量共同分析情資，以儘速於健診作業期間瞭解駭侵行為態樣、入侵方式、最早受駭時間、蒐集資訊種類與可能數量、與外部連繫情形及館處可能已洩露情資之評估等資訊；並審慎研擬管理層面或實務防制等建議作為，提供予館處及外交部資電處參用，俾提升外館處資安防護能力。

（二）製作健診結果會議簡報

健診結果會議簡報應於會議前製作完成，並於會議前提供館處相關主管紙本供參。依紐澳健診結果會議之模式，大綱分為：依據及目的、交付情資電腦查察、端點健診結果、中毒電腦分析、高風險程式、其他所見情形、建議事項等章節。

三、 健診結案會議

健診團隊應配合館處召開健診結案會議，以簡報方式向館處相關人員說明健診結果及改善建議，並協助回應館處人員資安問題，如屬決策性或涉館處管理問題，應交由外交部資電處統一回應。在結案會議前團員也會將發現的缺失部分立即協助改善，若無法現場改善的部分則會交由館處的資安官協助後續處理。

肆、 心得及建議

一、 心得

本次參與外交部之紐、澳線資安健診計畫，已協助外交部進一步強化我國駐紐、澳代表處資通訊設備之資安防護等措施。NCC 及 TTC 同仁依團隊任務分工，主要係針對物聯網設備網路印表機及其無線功能、對外網路連線品質等進行檢測，其次為網路設備、網路架構及上網資費進行評估，及協助團隊其他任務之執行(如進行端點檢測及惡意程式分析)。有關無線印表機預設開啟 WIFI DIRECT 功能或網路印表機預設帳號密碼無變更，及部分 VDSL 數據機的 WIFI 熱點功能開啟等狀態，皆於發現當下立即協助修正相關參數設定。

另發現部分館處專屬無線網路認證異常，或內網網路埠誤接導致不同屬性的網段串接在一起，可能造成網路不順或網段訊務異常等情勢，皆已在團長複核後立即修補，以避免資安風險擴大。

另團隊必須在短時間內找出受駭主機的受駭根因及將所見情形的改善建議等，撰寫出結案報告並提供給館處，都需要靠團隊成員的合作完成。而藉由不同團隊成員臨時任務編組及時分享彼此技術經驗，合力發現解決主機受駭及改善網路環境等問題，讓團隊成員一起學習解決資安健診所發現各層面的議題，皆有助於提升團隊成員及外館參與者彼此間的資安防護認知與能力。

二、 建議

NCC 及 TTC 同仁針對駐外館處租用當地電信事業之寬頻上網服務及連線品質進行清查，發現部分館處有頻寬擁塞或申請多條上網服務卻未充分應用等情形，已及時經團長反映給駐外館處參考改善。

另發現駐外館處之當地電信事業在提供我國駐外館處電話服務時，已有以網路電話(VoIP)取代傳統類比式語音電話或 ISDN 數位式電話的趨勢。但駐外館處對於資通訊設備連網及網路電話服務，卻有分別申請皆具上網服務之情形。因此，建議各駐外館處可盤點選擇使用 VoIP 電話服務時，得一併評估是否調整其租用當地電信事業提供寬頻上網服務及 VoIP 電話服務之網路架構及

上網速率選項，以降低整體資通設備連網風險及節省電信費用之支出。