１１０年度工作研究報告

題目：後疫情帶來的數位創新與資安威脅

撰寫人：單位　工程司

職稱　助理研究員

姓名　梁雁惠

☑有意願參加本部獎勵科技行政研究發展評獎(有意願者請打勾)

單位主管評語	近年來資安越來越受政府與企業重視，受到新冠肺炎影響，資安問題也變得複雜，本研究針對新冠肺炎疫前後的資安事件進行比較，歸納出疫後資安威脅，並給予政府、企業以及個人應對建議參考。
推薦參加本部獎勵科技行政研究發展評獎	（請打勾）
單位主管簽章	

備註:

一、報告內容以 10 頁為原則。

二、本篇工作研究報告，如參加本部獎勵科技行政研究發展評獎，請依本部獎勵科技行政研究發展作業要點規定辦理。

目錄

壹、 前言

一、 研究緣起與目的

資訊安全早在過去十幾年開始，就是一個較為敏感的議題，但國內大部份企業對於「資訊安全」意識並不高，由於難以預測未來的情境以及受到快速變化的環境所挑戰，無論是面對疫情來勢洶洶或是疫情下數位轉型帶來的資安危機，大多數企業仍然處於「被動反應」模式，針對單點事件或對應決策都是採取走一步算一步的態度。

今年初疫情進入三級警戒，國內有許多企業改採分流分區辦公，甚至是居家辦公，居家工作的環境不比公司辦公室環境嚴謹，工作需要參與視訊會議，則必須採用家庭網路及個人家用設備儀器進行會議，這也大大增加公司與人員資安防守困難，無法將防火線拉到所有人的家裡，這也就讓網路安全、設備安全等問題暴露在危險下，這些重要資訊包括公司、客戶資料、高階管理人員存取權、企業金流紀錄、專利技術等，若被有心人士掌握越多，影響及風險也就隨之擴大。

經過疫情肆虐一年的洗禮，**在後疫情時代，個人或企業都必須具備保護資訊的觀念**，並且確實的執行對應的防護措施，才能降低遭受惡意攻擊的風險。

二、 研究方法與過程

(一) 資料蒐集

- 參加資安沙龍或資安技術應用論壇與演講
- 廣泛閱讀資訊安全與技術分享相關讀物
- 蒐集疫情期間下的資安攻擊實例

(二) 專家交流

- 聆聽資安技術專家學者對於資安事件的看法
- 與專家學者討論資安因應措施與建議作法

(三) 分析彙整

- 將上述資料進行細部整理與分析

(四) 撰寫報告

- 撰寫後疫情資安威脅研究工作報告

貳、 何謂疫情資安威脅

一、 數位化資安威脅

資通訊科技發展迅速，帶動整體數位經濟蓬勃發展，在這個非常便捷的時代，我們可以透過網路完成許多的事物，不論是上網購物、轉帳、繳費、辦公、收發信、通訊等，都可以透過一台小小的連網手持式智慧型裝置完成，但這也將增加個人資料甚至是企業機密洩漏的風險，造成嚴重的損失及巨大的傷害。

通傳會在今年(110 年)2 月公告「109 年通訊市場調查結果報告」，此報告以 16 歲以上消費者為調查對象，藉由其通訊傳播使用行為，完整呈現需求面的消費態樣與市場資訊，調查結果顯示我國 16 歲以上民眾個人與家中成員目前使用中的手機總數量平均為 3.49 支，其中**家戶智慧型手機擁有率為 96.8%**，可連網比例達 92.4%，使用網路的比例達 89%，平均一週使用網路的總時數為 41.2 小時。

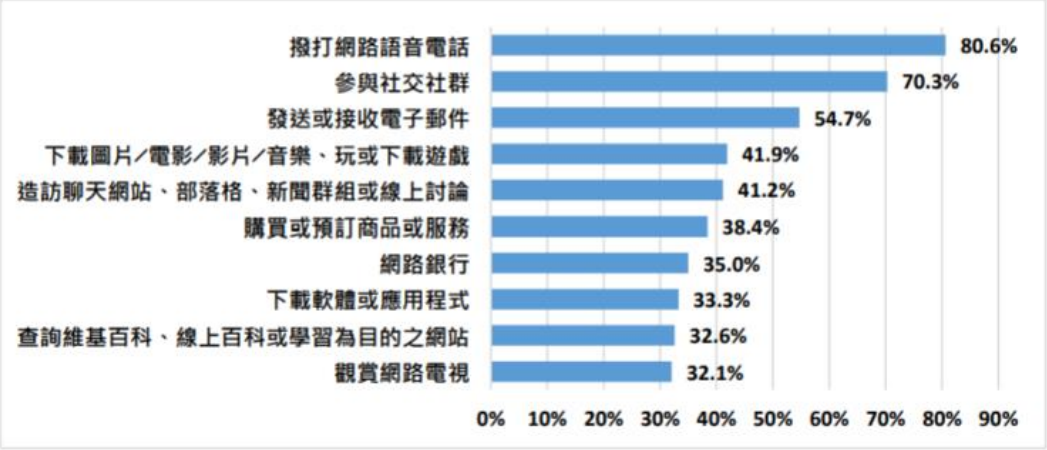

圖 1：民眾最近 3 個月內使用網路所從事的活動
(資料來源：通傳會，110 年 2 月)

此報告進一步揭露近三個月網路使用情形，發現**至少一天使用網路一次者，比例高達 92.9%**，其中，又以撥打網路語音電話、參與社交社群、發送或接收電子郵件等活動為大宗。

隨著行動通訊與寬頻網路普及，大幅度改變人們的生活模式，也因此間接地提供更多能夠讓有心人士下手的管道，他們可能藉由在社交社群軟體、電子郵件發送聳動標題的訊息，夾帶暗藏惡意程式的下載連結，讓人真假難辨而掉入陷阱；而網路電話的便利與免費優勢，其資訊系統的漏洞也可能讓不法人士未經授權盜撥付費電話、冒名通話甚至遭到竊聽，這些非常靠近你我的資安事件並非危言聳聽，人們依賴數位化生活越高，資訊安全就顯得更為重要。

二、 疫情資安問題興起

透過前一小節對於數位便利所帶來的資安威脅問題，已經可以很容易了解，在享受數位生活的同時，也潛藏著資訊安全外洩的風險，需要嚴防資安事件的發生。

資訊安全越來越受到各國政府以及企業所重視，2021 年 5 月 4 日**蔡總統**在出席 2021 臺灣資安大會開幕典禮致詞時，便指出「**疫情期間被廣泛應用的各種資通訊，未來將持續深入日常生活，加上萬物聯網時代來臨，更凸顯資安重要。**」。

圖 2：CYBERSEC 2021 臺灣資安大會

尤其在新冠肺炎（COVID-19）疫情爆發後，各國企業的工作模式大幅度改變，為了降低疫情對工作進度的影響，由原本的點到點辦公模式改為居家辦公或異地辦公，辦公行為模式的變異，縮短了上班與下班的界線，拉長了人與人之間的距離，加速企業對遠距工作的需求，擴大電子商務市

場，讓工作與私人生活的數位化落實得更加徹底，但**數位化猶如雙面刃，帶來便捷，也使得資安威脅更甚以往**。本小節將針對新冠疫情後所深化的資安問題分為「雲端服務安全」、「網路使用安全」以及「醫療系統安全」三方面進行探討。

(一) 雲端服務安全

雲端服務是結合雲端運算、雲端儲存、網路連線等的一項數位化服務，知名服務商包含 Amazon AWS、Microsoft Azure、Google Cloud…等。在個人服務應用上，常見的有基於瀏覽器的 google 雲端硬碟，最大好處可以**跨平台、跨裝置**，而在企業環境中，可以用在多分公司或分店的企業組織進行實體店面異地協作，不用設置很多主機，資料就能即時同步，買方能隨時查閱訂單、出貨、維修等資訊，賣方也能即時同步相關資訊。

疫情期間使得企業數位轉型得更加到位，為了讓絕大多數的員工可以在家上班，企業對於雲端服務的依賴更甚以往，多半將基礎設施環境與公司內部資料改架設至雲端環境，然而，移轉到雲端後，也出現了新的資安風險，其一為**一般企業內採用的雲服務可能來自於多家廠商**，所購買的雲服務又與企業內部環境的**身分存取管理並不是同一套，缺乏整合的身分管理較難以掌控與溯源**，可能遭到冒用取得企業內部機敏資料，另一大隱憂則是**員工使用私人設備或未受監督的應用程式來處理工作業務**，也大幅增加企業資安團隊監管難度。

(二) 網路使用安全

我們從前一節「數位化資安威脅」提到的通傳會針對 109 年通訊市場調查結果報告中，可以發現國人使用手機上網的比例顯然已是相當地高，**家戶智慧型手機擁有率為 96.8%**，可連網比例達 92.4%，**使用網路的比例達 89%**，平均一週使用網路的總時數為 41.2 小時。

然而，隨著 110 年 5 月疫情大爆發，指揮中心宣布提升全國疫情警戒至第三級後，大部分的企業皆受到強力波及，大多數非必要接觸之工作緊急轉為遠距辦公模式處理，學校教學也全數改為遠距上課輔導，工作、校園生活與私人生活的界線開始變得模糊，間接地也導致人們上網的時數增加。

遠距工作模式常需要搭配其他軟體(如虛擬私人網路 virtual private network，VPN)協作下進行(如下圖)，但企業內部網路所設置的防火牆、惡意程式偵測系統等資安防護措施，無法延伸到個人家用網路，員工頻繁使用 VPN 連線到企業內網，也讓**企業網管人員難以監控 VPN 是否出現異常活動**，有心人士便是趁此疫情升溫期間展開一波波惡意攻擊，若是內網遭到入侵，便可能造成企業機密資料外洩、破壞，甚至遭到駭客恐嚇勒索。

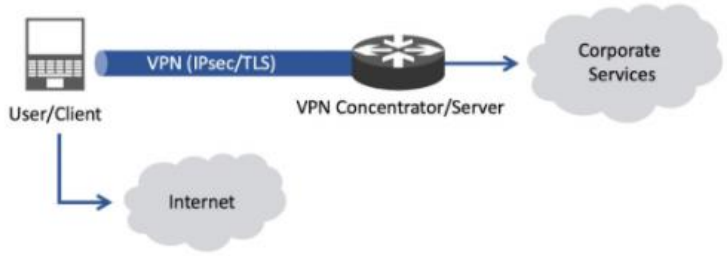

圖 3：遠距工作透過 VPN 虛擬私人網路進入公司
(資料來源：TWNIC，109 年 6 月)

除了企業內網遭到駭客入侵的問題相對增多外，對於一般民眾的社交工程攻擊也是相對提高，例如釣魚惡意詐騙活動增多、色情暴力內容廣告連結頻頻出現等，有些甚至以購物網頁偽裝，騙取個資、帳密、信用卡號，或是利用簡訊、電子郵件等通訊工具搭配較吸引目光的文字訊息，傳送釣魚網站連結或應用程式下載連結，致使受害人遭誘騙上當。

(三) 醫療系統安全

早在 2000 年衛服部就研擬電子病歷交換與整合機制，2011 年起建立「電子病歷交換中心」，使得任一間醫療院所、診所皆可透過 IC 健保卡取得病人的醫療紀錄，也能提供醫療機構上傳病人用藥紀錄、檢驗結果、影像報告、手術紀錄等診治相關資料，臺灣的醫療服務及健保制度，在全球獲得高度肯定與國際聲譽，但其擁有的**龐大醫療相關資訊與個人醫病隱私資料，定然也容易吸引有心人士的目光**。

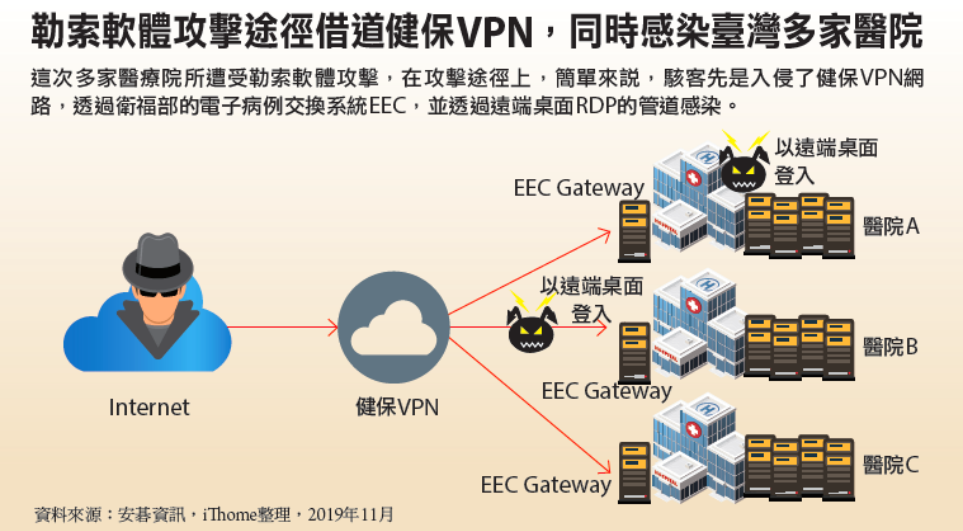

圖 4：勒索軟體攻擊途徑借道健保 VPN

(圖片來源：安碁資訊，iThome 整理，108 年 11 月)

本土疫情升溫，最受波及莫過於醫療院所，醫護人員除了要照顧收治患者，還需要避免出現院內感染個案，醫療院所與診所亦紛紛制定遠距醫療機制與服務規劃(如下圖)，期望利用數位化服務取代面對面接觸，然而，在人力吃緊的情況下，院內資安防護網也相對脆弱，**駭客的攻擊手法多如牛毛，例如常見的勒索軟體、木馬程式、殭屍網路、DDoS 攻擊等**，這些攻擊手法日益更新，複合式攻擊手段亦曾出不窮，防不勝防，面對疫情期間的醫療系統資安攻擊威脅，多數醫院皆措手不及，醫療院所在承擔巨大的個資外洩風險下，往往容易向惡勢力妥協而支付贖金，這也使得駭客更加猖狂。

圖 5：遠距醫療服務流

(資料來源：2020 智慧醫療研討會，CIO Taiwan 剪輯，109 年 8 月)

參、 研究發現與後疫情資安事件案例

在本研究前一章提到一些疫情後興起的資安問題,包含雲端服務安全、網路使用安全以及醫療系統安全等問題，此些問題疫情發生之前，最常聽聞大型企業、大型醫療院所機敏資料遭駭，被駭客集團高額重金勒索，其實，**中小型企業與小型診所才是駭客集團的最愛**，因為中小型營運機構多半有以下缺失：

- 缺乏資安意識
- 內部人員訓練不夠落實導致操作不良
- 沒有準備一定程度的資安預算
- 沒有組建資安團隊為企業設置資安防護
- 公司營運系統未委託專業團隊建置導致漏洞或後門多
- 購買中國大陸製軟硬體設備
- 系統權限控管不佳

加上臺灣產業結構多以中小型企業為主，其資料庫中具有大量有價值的個人資訊，是故駭客的目光較多鎖定在中小型企業，這類型受害企業通常被駭客勒索小金額，企業主為了避免影響到顧客信任度，多半會付錢以息事寧人，也讓一般民眾無法知曉警惕，進而助長了這類型犯罪事件的發生。

以下便針對疫情後，因遠距工作與企業數位轉型所可能帶來的影響，探討較為典型的資安事件，分為「VPN 虛擬私人網路外洩事件」與「雲端資料外洩事件」來進行探討。

一、 VPN 虛擬私人網路外洩事件

前一章小節便有提到健保 VPN,事實上健保 VPN 就有點類似目前的遠距工作模式，所有連回衛服部的電子病歷交換系統就如目前的公司主機，而所有加入健保之醫療院所便是現行的遠距工作者，而它的運作機制主要

是在公共網路上架設一條虛擬的加密資料通道，家用電腦會與遠端伺服器交換金鑰，來確保資料的隱蔽性，避免被竊取。

新冠疫情造成的全球人口死亡數變相加速企業轉型，越來越多人採取在家遠距辦公模式，然而，住家資安防護措施相較脆弱許多，且部分家用電腦裝設的並不是正版作業系統，甚至沒有裝設防火牆或任何防毒監控軟體；在疫情期間，多數在家工作者會透過 VPN 虛擬私人網路連回公司，而**連線 VPN 之後，所有的上網數據都會經過 VPN 伺服器，並且留存一些上網紀錄，例如姓名、電話、地址、帳號密碼、信用卡號、IP 位置等涉及隱私、資安、財產安全等訊息**，若使用不良 VPN 服務商釋出的免費 VPN 軟體，還可能遭到不法人事惡意蒐集與販售這些上網用戶的隱私訊息。

專門評測 VPN 伺服器性能的 vpnMentor 於 109 年 7 月便揭露 7 家位於香港的 VPN 供應商服務，聲稱不會留存用戶連網紀錄(no-log policy)，並提供軍用等級的安全功能，但卻均將用戶隱私流到一個未設置資安防護的共享伺服器上，資料量高達 1TB 以上，包含未加密的帳號密碼、付款訊息、使用者電子郵件、姓名/電話/居住地址，影響約 2,000 萬人權益，而在事件發生後的 10 日內，供應商便關閉 VPN 伺服器，但潛在影響仍可能會有欺詐、人肉搜索、勒索、病毒式攻擊以及黑客攻擊等問題存在。

Data Breach Summary

Apps	UFO VPN, FAST VPN, Free VPN, Super VPN, Flash VPN, Secure VPN, Rabbit VPN
Headquarters/Location	Hong Kong
Industry	Cybersecurity
Total size of data	1.207 TB
Total number of files	1,083,997,361 records
No. of people exposed	Over 20 million, based on user numbers claimed by the VPNs
Geographical scope	Worldwide
Types of data exposed	Activity logs, PII (names, emails, home address), cleartext passwords, Bitcoin payment information, support messages, personal device information, tech specs, account info, direct Paypal API links
Potential impact	Fraud, doxing, blackmail, extortion, viral attack, and hacking, arrest, and persecution
Data storage format	ElasticSearch Server

圖 6：vpnMentor 針對 7 家 VPN 供應商服務揭露資料外洩事件
(資料來源：vpnMentor，109 年 7 月)

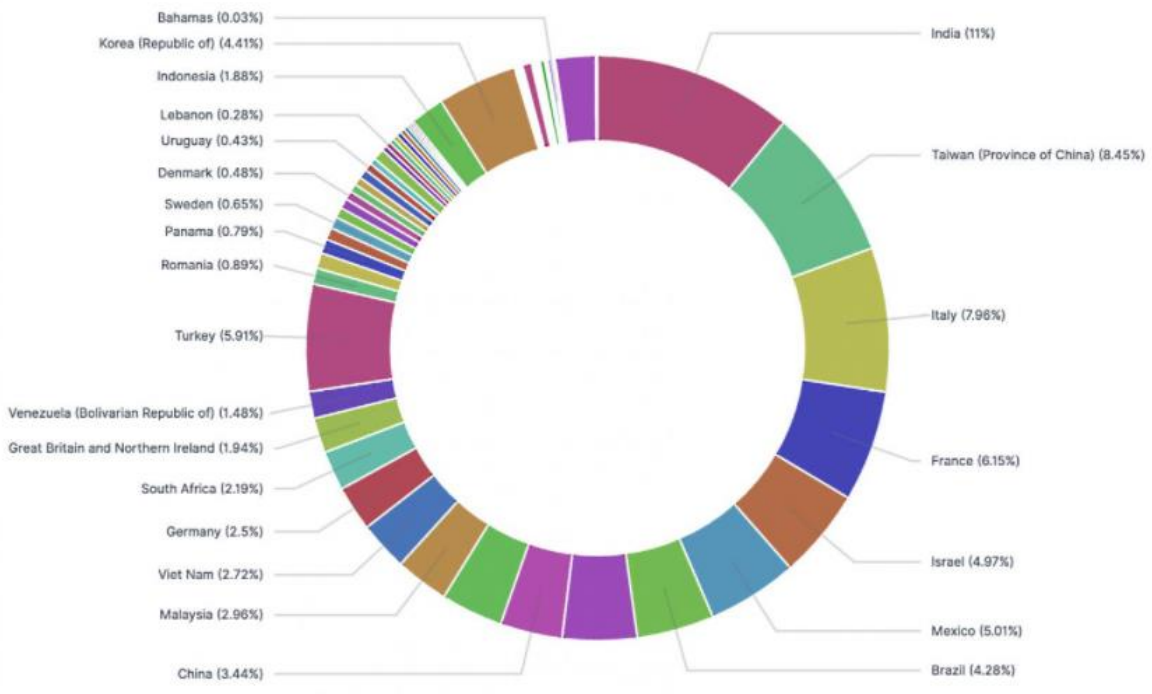

圖 7：某跨國 VPN 伺服器資料外洩各國影響程度評估
(資料來源：BleepingComputer，110 年 9 月)

今年(110 年)9 月資安媒體 BleepingComputer 也揭露，駭客利用跨國 VPN 供應商服務軟體漏洞，蒐集 50 萬筆 VPN 使用者帳號密碼，並公布於 RAMP 黑客論壇、Groove 數據洩漏站點等暗網中任人使用，影響 1.2 萬台裝置設備，影響範圍遍及全球數個國家，其中，臺灣為受影響嚴重程度第二受災戶(第一為印度)，值得國內企業在使用這些 VPN 服務時謹慎考量，而在事件發生後，該跨國 VPN 供應商便緊急修補漏洞，但其所存放的帳號密碼顯然已外洩，使用者若不即時異動密碼，則仍有被冒用的風險。

如此好用的 VPN 為什麼突然在疫情期間失控？主要還是負載的問題，過去非疫情期間主要以業務緊急性來短暫、少量、少次的透過 VPN 取得遠端伺服器的資料，但**疫情期間，透過 VPN 連回網路的人數多、頻率高、時間長度長都成為常態，造成系統負載壓力過重**，使得使用者現況執行的動作、登入的裝置等都難以監控，也難以辨別異常情形，因此，駭客集團便利用新冠疫情製造資安災情，各種 VPN 攻擊手法紛紛出爐，使得企業對於 VPN 又愛又怕。

二、 雲端資料外洩事件

雲端資料外洩新聞時有耳聞，由於企業對雲端服務的接受度與日俱增，但在僅關注於數位轉型的同時，並**未將雲端管理存取權限相關的安全機制徹底落實**，導致儲存在雲端機敏資料無意中遭到公開，任人取用。

對於一般民眾而言，國內新聞大肆報導的 iCloud 外洩事件，敲響了第一聲警鐘，103 年 iphone6 發布會前夕的蘋果雲端 iCloud 外洩 60 張美國女星私密照事件，沒有影響到 iphone6 的銷量，卻造成 101 位女星名譽損害；107 年至 108 年 Facebook 曾因網站上的電話查詢功能漏洞遭駭，外洩 5 億多筆個資，其中多達 73 萬筆為台灣用戶資料，雖然立即修補漏洞，但此些個資仍在 109 年被人放在駭客論壇中販售；108 年至 109 年 1111 人力銀行與 104 人力銀行都相繼遭到中國駭客入侵，將數百萬筆個資放到暗網販售，此些事件似乎都可以看出越龐大的資料庫，越容易吸引到駭客的目光，因此，需要有更良善的資安保護機制。

然而，駭客手法層出不窮，疫情的驅使下，企業紛紛投入數位轉型的行列，因此所面臨的雲端風險更高，而提到雲端，便要提到 Linux 作業系統，因為 Linux 作業系統可說是除了桌上型電腦所使用的 Windows 以外，各種廣告刊版、大型銀幕、各類網站主機都是採用 Linux 作業系統，甚至是 MacOS 與 Linux 皆基於 Unix，設定都一樣，Andriod 系統的內核也同樣採用 **Linux**，**其應用廣度極高，讓駭客集團使出各種方式攻擊**。

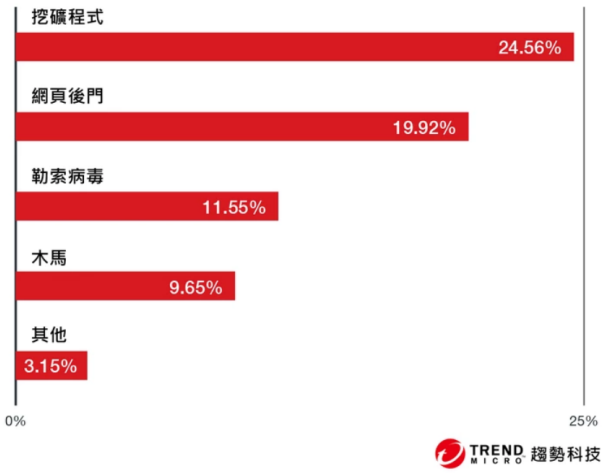

圖 8：趨勢科技 2021 上半年 Linux 資安研究報告揭露駭客手法
(資料來源：趨勢科技，110 年 9 月)

今年(110 年)國際知名資安廠商趨勢科技針對上半年 Linux 資安現況發表相關調查報告，報告指出 **Linux 作業系統正在持續受到攻擊，其中偵測到挖礦程式、網頁後門及勒索病毒占惡意程式中的 56%**，所揭露的事實讓人相當驚訝，而最值得注意的則是，大部分的公有雲都是基於 Linux 作業系統運作，現今許多 IoT 裝置與雲端應用程式或技術大多都基於 Linux 作業系統進行開發，故此份調查報告所揭露的問題，將大幅度影響各產業考慮使用雲端來維護內部重要且機敏資料的必要性。

2021 年再次應驗了趨勢科技臺灣區暨香港區總經理洪偉淦所說的「 **2020 年在疫情影響下，加速企業數位轉型的進程，企業將可能面臨雲端風險升高與逐漸成長的複合式目標攻擊 。**」

肆、 研究建議

在這個非常便捷的時代，我們可以透過網路完成許多的事物，無論是線上購物、網路辦公、網路通訊等等，幾乎所有資訊都能透過網路傳遞與分享，但往往一不小心就有可能洩漏個人資料或企業機密，造成嚴重的損失及巨大的傷害。近年，各種駭客攻擊手法層出不窮，小則個人資料外洩而被詐騙、大到企業機密被竊取，遭到勒索損失大筆金錢的新聞，在全球各地不斷地發生，都在提醒我們要更小心的使用網路服務與保管重要資料。

經過一年多以來的新冠肺炎疫情洗禮，面對後疫情時代資安威脅，大型企業與機構嚴陣以待，中小型企業與個人也要堅守防火線，杜絕駭客集團猖獗的機會，期望能夠呼籲政府與企業，甚至個人都能重視資安防護的重要性，本研究歸納以下幾點建議：

對政府與企業的建議：

1. 聘任具有洞察威脅能力之資安專業人員。
2. 擴大單位內 IT 人員的職責範圍，將防禦線拉大。
3. 設法將資安意識導入在學與在職各領域群體。
4. 明定遠距工作指引及措施，並確實落實與掌控。
5. 強化雲端資料中心防護，分層權限管控。

6. 採取零信任策略，全天候偵測威脅來源，並提早警示。

對個人的建議：

1. 減少使用公共場所免費 Wi-Fi 連網，避免遭到入侵。
2. 務必要重視雲端安全，盡量避免將重要資料擺放置免費雲端。
3. 確實遵守服務單位所實施遠距工作指引及措施。
4. 拒絕使用非法、盜版、免費等來路不明軟體。
5. 定期檢視防毒軟體更新，並全天候開啟偵測惡意病毒。
6. 防備社交工程、網路釣魚，審慎點選不明連結或下載不明檔案。

伍、 參考資料

1. 109 年 11 月 4 日 5G 時代下的資安防禦新思維論壇(新竹)
2. 110 年 5 月 4 日-6 日 CYBERSEC 2021 臺灣資安大會(台北)
3. 110 年 9 月 3 日 SP-ISAC 資安沙龍線上論壇，https://www.nchc.org.tw/Active/ActiveView/493?mid=47&page=1
4. 110 年 9 月 28 日重建高生產力與低風險網路辦公環境線上講座，https://www.netadmin.com.tw/files/event/20210928event/index.html
5. 110 年 10 月 13 日零信任網路存取技術線上研討會
6. 109 年 8 月 23 日 2020 智慧醫療研討會(台北)，CIO Taiwan 剪輯影片 https://www.youtube.com/watch?v=dQis48vRtR4&t=2s
7. https://www.vpnmentor.com/blog/report-free-vpns-leak/
8. https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/
9. https://www.ithome.com.tw/security
10. https://www.netadmin.com.tw/netadmin/zh-tw/
11. https://www.informationsecurity.com.tw/article/article_detail_2021.aspx?aid=9063
12. https://udn.com/news/story/7240/5766920