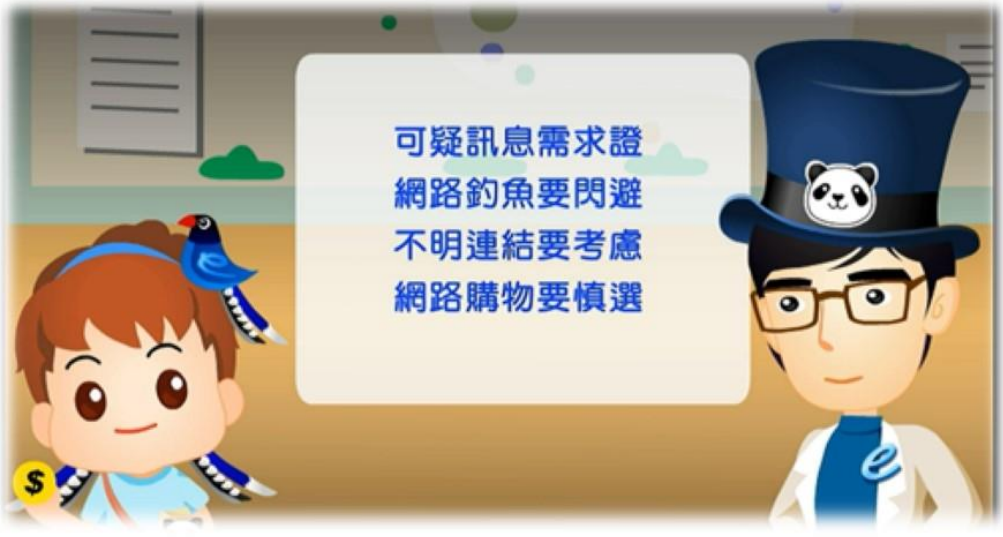
公務機密

資訊安全維護



盡量勿下載來路不明的軟體，
以避免惡意軟體的侵入。

資安時事案例

專家帶路：遠端辦公網路安全3大策略

一個小動作「個資恐外洩」！外媒警告Google、臉書帳號綁定登入第三方要小心

個人資料保護法

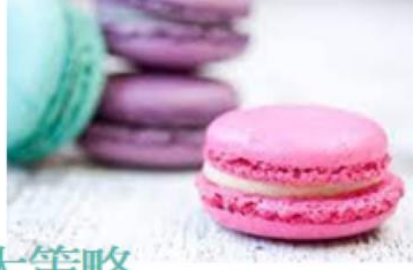
淺談個人資料保護法-購屋篇

維護宣導

面對勒索病毒- 資安防護該怎麼做?

數位學習

103年度資安動畫金像獎
上傳決定害死你



專家帶路：遠端辦公網路安全3大策略

資安人 2022 / 11 / 14 編輯部

自新冠肺炎(COVID-19)疫情以來，遠端工作模式已是許多上班族的常態。但礙於時間緊迫或建置成本等因素，IT人員在建置遠端工作環境的過程中，有可能因為疏忽，而產生網路安全的漏洞。這些漏洞若沒有即時發現及處理，很有可能被有心人士或駭客利用，公司內部的重要資料與機密資訊，將可能會暴露在風險當中。

近期案例中，發現某公司防火牆的Log訊息中，一台虛擬機定時對內部網路進行端口掃描，追查發現為開發人員為了方便在外出差遠端工作，在公司內部建立虛擬機，並使用TeamViewer遠端軟體，方便存取公司內部系統服務。我們對該虛擬機進行足跡分析後，發現疑似與官方公布漏洞CVE-2020-13699相關。該漏洞主要是駭客利用TeamViewer未適當處理URI的使用限制，駭客可以在URI值中嵌入惡意資料，誘使受害者點擊後，連回惡意Web網站並自動開啟遠端電腦的共享SMB服務。在開啟SMB服務後，Windows 會開始執行NTLM身分驗證請求獲取相關訊息，駭客則由遠端利用工具伺機竊取SMB分享內容，有機會取得受害者的系統登入密碼，並進行暴力破解。

該漏洞是屬於Unquoted URI handler，影響範圍URI handlers teamviewer10, teamviewer8, teamviewerapi, tvchat1, tvcontrol1, tvfiletransfer1, tvjoinv8, tvpresent1, tvsendfile1, tvsqcustomer1, tvsqsupport1, tvvideocall1, and tvvpn1。

針對上述案例，NEITHNET專家提出以下三大防範策略，一旦威脅入侵，能即時中斷駭客Kill Chain，在攻擊初期即可阻斷，防止駭客拿取控制權、竊取帳戶密碼，協助企業建立完整的遠端辦公網路安全。

策略1：內網異常行為辨識

NEITHViewer主要針對內部網路異常行為辨識，不僅可以偵測內網掃描行為，更可以提供弱點攻擊偵測能力，當駭客進行TeamViewer弱點攻擊時，NEITHViewer則會觸發EXPLOIT TeamViewer .iFrame Observed (CVE-2020-13699)事件，並能同時告警管理人員，即時處理惡意連線行為。

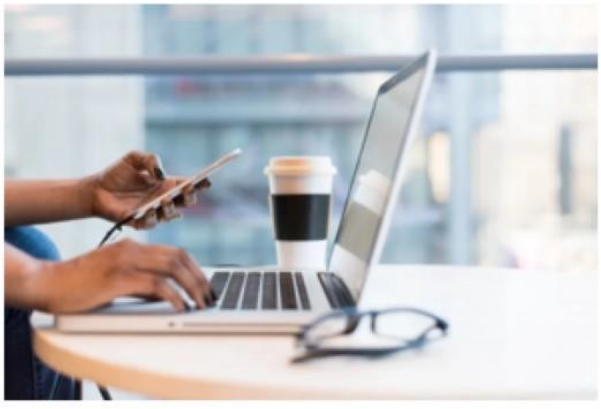
策略2：惡意網址檢測

以上述案例，當User無意點擊含有駭客設置的惡意Web網站時，透過NEITHDNS的DNS過濾惡意網址檢測功能，可以進行即時阻擋，防止User連至惡意Web網站後，在不知不覺中已被駭客入侵，被當成駭客入侵的跳板，甚至洩漏公司機密。

策略3：端點安全防護

運用NEITHSeeker MDR系統，找出端點內可能被安裝未更新且已有弱點的遠端控制軟體，如TeamViewer、Webex等，提醒管理者需要針對該軟體進行更新。此外，藉由NEITHSeeker提供即時情資比對，可即時告警該台電腦正在連線惡意Web網站，並由專家即時告警並且關閉該程式，避免端點被駭客侵入造成機密資料外洩。

一個小動作「個資恐外洩」！
外媒警告Google、臉書帳號綁定登入第三方要小心



Yahoo 3C大事紀 2022.11.3 （文：費司特、圖：pexels）

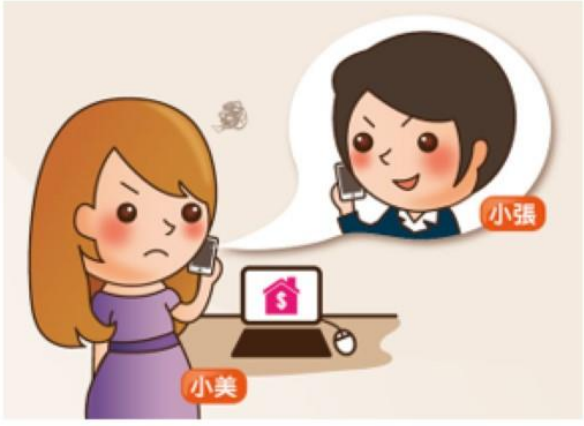
大家平常進入第三方平台網站或使用APP時，只要選擇Google或臉書帳號登入，就可以免去重新註冊的手續，節省寶貴的登入時間，但是其實這樣的小動作存在著相當大的風險，一旦選擇綁定登入，很有可能導致你的個資外洩，得不償失喔！

根據《華盛頓郵報》報導，臉書曾警告用戶，目前有超過400個惡意設計的APP，故意讓用戶選擇使用臉書帳號登入假網頁，並從中竊取大量個資，造成用戶財務上的損失。日前有讀者向《華盛頓郵報》投訴，他曾在求職網站「iCIMS」按下「以Google帳號登入」同意選項，以節省登入和上傳履歷的時間，但網站卻私自盜取求職者在Google雲端硬碟內的所有檔案，其中可能包括照片、影片等私密的個人資料，此外，還有民眾指出，網路論壇「Reddit」也是用同樣的方式來取得用戶的大量個資。

對此，iCIMS發聲明表示，並未在用戶上傳履歷時查看用戶Google帳號的檔案和其他資料，Google公司則回覆《華盛頓郵報》，用戶在「使用許可」選項中可以選擇哪些檔案資料能分享、保有控制權，但是有多少用戶會去閱讀、理解冗長的授權條款呢？

因此，《華盛頓郵報》建議，為了避免惡意網站、各大公司取得個資和檔案權限，只要看到「是否以Google或臉書帳號登入或註冊」的選項，最好一律跳過，不要按下「同意」，以免你的個資落入不法之徒手中！

淺談個人資料保護法



【文 / 鍾運凱】

案例

小美在網路上刊登廣告，要出售自己名下的房屋，並公開連絡電話。房仲的業務員小張看見這則廣告，於是打電話詢問小美，是否願意委託他的房仲公司賣房子，小美拒絕。沒想到，接下來幾乎每天都有房仲公司打電話來詢問，小美覺得很煩。試問，房仲人員打電話的行為，是否違反個人資料保護法？

一、 何謂個人資料？

所謂「個人資料」是指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

二、 當事人對於個人資料的權利為何？

當事人對於他人持有自己的個人資料，得查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理或利用、請求刪除等權利。

三、 如何才能合法蒐集他人個資？

首先必須有合法的特定目的，例如仲介為了銷售房屋而蒐集屋主的資料。此外，必須有下列情形之一：

1、法律明文規定可以蒐集
2、與當事人有契約或類似契約之關係
3、當事人自行公開或其他已合法公開之個人資料
4、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或

蒐集者依其揭露方式無從識別特定之當事人

5、經當事人書面同意
6、與公共利益有關

如果是業者「直接」向當事人蒐集其個人資料，蒐集時須盡告知以下事項：蒐集者的名稱；蒐集之目的；個人資料之類別；個人資料利用之期間、地區、對象及方式；當事人得行使之權利及方式；當事人得自由選擇提供個人資料時，不提供將對其權益之影響。但如果不是直接由當事人提供之個人資料，蒐集時則不需要告知上述事項。

此外，有下列情形之一者也無須告知：依法律規定得免告知；業者履行法定義務所必要；告知將妨害公務機關執行法定職務；告知將妨害第三人之重大利益；當事人明知應告知之內容。

四、 如何才能合法利用他人個資？

業者合法蒐集的個資，只要在合法的特定目的範圍內，都可以利用。但如果要在特定目的外去使用個資，則必須符合以下情形之一：

1、法律明文規定；
2、為增進公共利益；
3、為免除當事人之生命、身體、自由或財產上之危險；
4、為防止他人權益之重大危害；
5、經當事人書面同意。

業者在處理、利用他人個資時，如果該個資是業者直接向當事人蒐集而來的，不需要另行告知；但如果是間接蒐集的個資，必須告知以下事項：一、個人資料來源；二、公司名稱；三、蒐集之目的；四、個人資料之類別；五、個人資料利用之期間、地區、對象及方式；六、當事人得行使之權利及方式。

此外，業者將他人個資作特定目的外的利用，則必須告知當事人其利用目的、利用之範圍及同意與否對其權益之影響。

五、 業者對個人資料有甚麼義務？

業者對於持有他人個資，應盡以下各項義務：

1、應維護資料之正確，並應更正或補充之
2、個人資料正確性有爭議者，應停止處理或利用
3、個人資料蒐集之特定目的消失或期限屆滿時，應刪除、停止處理或利用該個人資料
4、違法蒐集、處理或利用個人資料者，應刪除、停止蒐集、處理或利用該個人資料
5、因可歸責於業者之事由未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象
6、個人資料被竊取、洩漏、竄改或其他侵害者，應查明後通知當事人
7、業者受理當事人以上各項請求，應於十五日內處理完畢

此外，業者保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏，而且主管機關得指定業者訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

所謂適當之安全措施，應包括下列事項：

1、配置管理之人員及相當資源。
2、界定個人資料之範圍。
3、個人資料之風險評估及管理機制。
4、事故之預防、通報及應變機制。
5、個人資料蒐集、處理及利用之內部管理程序。
6、資料安全管理及人員管理。
7、認知宣導及教育訓練。
8、設備安全管理。
9、資料安全稽核機制。
10、使用紀錄、軌跡資料及證據保存。
11、個人資料安全維護之整體持續改善。

六、 結論

由以上說明可知，現行的個資法對個人資料保護可以說是相當嚴密，對於合法蒐集、利用他人的個資，也有相當明確的規範。此外，如果是自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料，或者於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料，例如網路上他人分享的影片，這些情形都可以不適用個資法，以免阻礙資訊的流通。

案例中，小美的電話號碼是自行在網路上公布的，屬於上述「當事人自行公開的個人資料」，小張或其他的房仲公司只要在合法的特定目的範圍內，並且盡到告知義務，就可以合法地利用，且須有安全措施保護該項個人資料。如果小美表示拒絕接受行銷時，房仲人員就應該立即停止利用其個人資料，並且刪除之。

面對勒索病毒

資安防護該怎麼做?

新聞事件

109年5月4日至5月5日間，國內多間重要能源及科技公司如中油、台塑及記憶體封測廠力成接連傳出遭勒索病毒攻擊，駭客入侵並將勒索軟體植入公司系統、個人電腦以及伺服器等資訊設備，造成重要檔案無法開啟、系統停擺，同時公司也被要求交付贖金。三間公司都緊急要求員工關機斷網，其中中油的捷利卡、車隊卡及中油PAY等支付工具皆被迫暫停使用，直接影響顧客權益。

經過調查局調查，駭客是在數個月前透過員工的個人電腦、網頁以及資料庫伺服器，入侵企業內部網路並展開刺探與潛伏，等待竊取帳號權限後侵入網域控制伺服器，並利用凌晨時段竄改群組原則（GPO）以派送具有惡意行為的工作排程。當企業員工打開電腦則會立即套用 GPO 並執行該工作排程，等到核心上班時段，駭客預埋在內部伺服器中的勒索軟體自動下載至記憶體中執行，當檔案加密成功就會顯示勒索訊息以及聯絡用的電子信箱。

病毒特色

能夠針對特定時機發動攻擊，也彰顯了此類駭客攻擊的特色：**事先潛伏、伺機而動**。「許多勒索軟體其實早就潛伏在企業網路裡部署，等時間到了再同時發動，讓破壞效果更大。」

勒索病毒入侵的途徑相當繁雜，有可能是員工慎點選了釣魚郵件、遭感染的USB被插入公司電腦、也可能是駭客透過軟體漏洞植入惡意程式。在順利進入企業內網後，駭客會試圖破解AD（網域控制伺服器）或者具備派送功能的資產管理軟體權限，將病毒擴散到轄下的各台電腦後伺機潛伏。

因應措施

要防範勒索病毒，在事前就必須做好資料備份及異地備援、將備份資料做加密，並在發現病毒的當下防止感染擴大，儘快關機斷網，保留證據讓鑑識單位分析。

一、安碁資訊整理七項資安重點防範措施，說明如下：

1.確實保護AD管理者，加強密碼強度、管制登入位置。
2.加強備份，確實執行弱點補強。
3.確認所有防火牆設備的規則管理、嚴格限制外部遠端桌面協定（RDP）相關設定。
4.檢查整體網路架構，是否有未經允許或遺漏的線路，可能造成外對內連線的風險。
5.確認主機管理帳號是否存在弱密碼，如鍵盤組合（1qaz2wsx等）、常見的弱密碼（Passw0rd等），若有立刻更改。
6.掌握單位內防毒軟體是否安裝及更新情況，未安裝或更新異常應立即處置（以中油事件為例，趨勢防毒從849版以後病毒碼皆可偵測）。
7.網路上的芳鄰共享資料夾建議盡量不使用，如要使用應設定密碼存取，避免遭惡意程式存取利用。

二、知名資安大廠賽門鐵克之諾頓提供七大要點，督促人們要防患未然，說明如下：

1.不要支付贖金。支付贖金只會變相鼓勵勒索病毒背後的駭客，而且即便支付了贖金，也無法保證你能取回遭到加密的資料。
2.從你信任的備份資源取回檔案。這是最快能夠重新取回檔案的方法。
3.避免在電子信件、電話、簡訊中提供自己的個人訊息。常見的招數包含利用IT管理員的身份騙員工下載惡意軟體，所以當接到可疑來電時，記得與公司內的IT部門再次確認。
4.使用有保證的防毒軟體，並隨時保持在最新的更新版本。
5.在電子信箱中採用內容過濾的套件，任何信件都該經過掃描、防止可疑的附件檔案滲透進電腦。
6.隨時更新電腦系統與軟體。這是能夠最有效防堵勒索軟體的方法之一。
7.在外旅遊使用公共wifi要特別留意，並記得通知IT部門。連線時確保自己透過可信任的VPN進行連線。