疫情時期之資安風險態樣與因應

文／施弘文 資訊工業策進會科技法律研究所專案經理

突如其來的新冠疫情，影響了全球的經濟與生活形態，政府機關及企業的防疫措施，改變了我們原有的工作及生活方式，除了各國於疫情期間陸續關閉邊境或對外停航外，限制外出、居家檢疫與隔離等措施，亦成為各國對內之防疫手段。而在因應新冠疫情期間，網際網路中另一種無形的風險威脅亦逐漸蔓延，正由於疫情期間各國或企業所採取之防疫措施，造成網路通訊的需求與個人在線時間大幅增加，而企業因應疫情實施遠距工作方式，其網路連線、部署及相關網路設備服務之使用，均提升了潛在之資安風險。

由於COVID-19疫情所帶來的不安與不確定性，使駭客有了可乘之機，依據Check Point資安公司從2019年12月底至2020年4月中，在全球所檢測到與冠狀病毒有關的網絡攻擊統計顯示，

“這期間包含網站含有「CORONA」或「COVID」之域名，或檔案文件、電子郵件中含有CORONA或新型冠狀病毒相關主題附加文件之網路攻擊，自4月以來大幅增加，平均每日達14,000次，為之前平均每日攻擊次數之6倍，而自4月第一週後，平均每日攻擊次數更上升至20,000次之多，而其中大部分之網路攻擊多屬於網路釣魚，並透過行動通訊裝置或手持設備實施。”

由此可知，在此波疫情下所面臨之資安威脅更加嚴峻，而就疫情所產生的資安威脅亦衍生出不同之態樣，除了較為常見以COVID-19或疫情相關為主題之網路釣魚郵件、假新聞及惡意應用程式或更新外，在因應疫情而轉變工作、生活形態所衍生之資安風險及駭客惡意入侵竊取資訊之資安威脅，亦成為COVID-19疫情下，企業或個人亟需納入資安風險考量之一環。

由於疫情影響，部分企業因實施遠距工作方式，相關之工作訊息、資料的傳遞均透過網際網路，而端點所使用之VPN連線、視訊會議系統、即時通訊軟體、工作協作平台等，均可能隱藏相關之資安風險。此外，駭客以惡意入侵方式而獲取病毒相關之傳播資訊、管制措施、疫苗研究、病毒之病理研究資料，以作為其他商業用途、財務勒索或阻礙防疫措施之進行，其所產生之影響，更將難以估計。

依世界經濟論壇於今年5月所公布COVID-19風險報告顯示，約有半數企業擔心因工作型態轉變導致網路攻擊與資料詐欺事件之發生此波疫情下企業第三憂慮之問題。而在目前疫情逐漸獲得控制的同時，此次的防疫經驗應可提供企業或個人在資安風險管理上不同之思考向。企業或個人除了可在技術面如對於原有之網路環境、架構、端點或連線強化其安全需求，如使用多因素之認驗證機制進行登入、強化有密碼強度、加強端點登入之安全性等外；在管理面上，企業亦可檢視其原有之資安風險管理規劃，將此種因疫情或不可抗力等因素而造工作、生活形態轉變所可能產生之資安風險納入安全維護計畫，並檢視其端點管理方式、通報應變措施及資料存取機制是否足以因應此種安風險，以提升企業之資安防護能量。

上稿時間： 2020年07月07日

新聞來源： https://view.ctee.com.tw/business/21090.html

文章標籤