清流月刊中華民國九十八年六月號

當發生資安事件時，首先應冷靜下來，嘗試了解事件發生原因、蒐集事件相關資訊並掌握可能影響範圍。

如何做好資安事件通報應變

◎ 劉建良

壹、緒論

為能有效掌握資通訊及網路系統在遭受破壞、不當使用等資通安全事件發生時，可以迅速掌握受害情形並進行應變處置，讓遭受影響的系統於最短時間內回復，確保業務之正常運作，國家資通安全會報於民國98年2月頒布國家資通安全通報應變作業綱要，明確律定資安事件影響等級定義及作業程序，與資安事件發生時通報和應變的作業流程。因此，如何依循作業綱要之規定，於發生資安事件時，迅速完整地做好資安事件通報應變，快速回復業務的正常運作，已是現今資訊從業人員皆須了解的重要議題。

貳、通報作業

發生資安事件時，往往讓人一時慌了手腳，不知該如何下手處理整起資安事件，導致無法迅速控制事件之損害。因此，當發生資安事件時，首先應冷靜下來，嘗試去了解事件發生原因、蒐集事件相關資訊並掌握事件可能的影響範圍，好讓接下來的通報作業能順利進行；接著透過與廠商、網管人員討論事情徵狀，推敲事件原因，進而確認事件成因並防堵其他相關的弱點，同時在處理事件過程中隨時回報內部長官有關事件之發展情勢，才能有效控管資安事件。

除了組織內部進行管控外，在通報作業中很重要的一環，就是透過國家資通安全通報應變網站(http://www.ncert.nat.gov.tw/)進行事件情資的通報與分享。該通報應變網站提供各政府機關(構)一個記錄資安事件的平台，各機關的資安聯絡人可透過這個平台，依循國家資通安全會報通報與應變作業流程(詳見圖1)，將遭遇的資安事件陳報相關單位，並視情況申請技術協助，俾能掌握資安事件處理時效。而通報機關的主管機關，也可經由網站通報資料的處理狀態，有效協助通報機關快速復原事件所造成的影響。因此當進行資安事件通報時，應先搜集事件相關資訊，確切掌握受影響的系統資訊(如IP位置、作業系統、作業系統版本等)，以及各種已裝置的安全機制(如防火牆、入侵偵測系統等)，接著對事件的影響及衝擊範圍進行適當評估，同時將初步了解的損害程度及事件的相關資訊(如遭影響時間、範圍等)記錄於通報應變網站之事件通報單中。

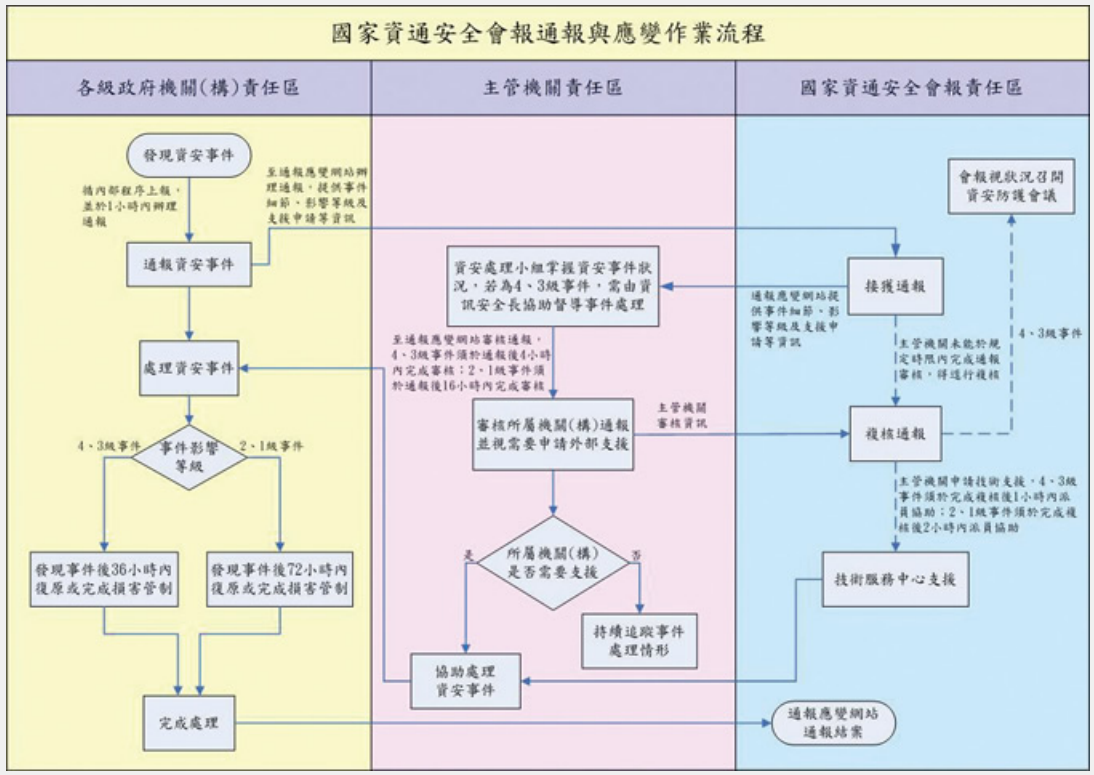

圖1 國家資通安全會報通報與應變作業流程

由於每起資安事件通常不只影響單一層面，評估資安事件影響範圍時，應做全面性的考量。在國家資通安全通報應變作業綱要中，為了能對事件影響等級有適當的量化指標，乃將資安事件分為三個面向進行衡量，分別評估該起資安事件對「機密性」、「完整性」、「可用性」三個面向所造成的衝擊；三個面向衝擊將依事件影響程度由輕至重區分為1級、2級、3級與4級，區分準則詳見圖2。藉由上述各面向等級之評估，可用以衡量整體資安事件實際造成的影響，並以其中衝擊等級最大之面向，做為整起資安事件之影響等級。

圖2 資安事件影響分級判定步驟

另外在國家資通安全會報通報與應變作業流程中規定，若判別事件影響等級後，應依不同資安事件影響等級投入資源進行事件處理。對於影響等級評定為1、2級的資安事件，應於事件發現後72小時內復原或完成損害管制；影響等級評定為3、4級的資安事件，應於事件發現後36小時內復原或完成損害管制。在完成事件處理後，則應儘速至國家資通安全通報應變網站完成通報事件結案作業，說明事件解決辦法以及解決時間，以確切掌握該次事件之處理情形。

參、應變作業

由於資安事件往往來得突然，若平時未能發展出一套完整的因應方案，則事件發生時就會手足無措，因此各級政府機關(構)應建立一套資安事件之事前安全防護、事中緊急應變及事後復原作業機制，在資安事件發生時才能快速進行應變處置。

一、事前安全防護：事前安全防護包含預防計畫，及對軟硬體系統設施、環境、人員培訓等之相關防護措施。

1. 藉由訂定防護計畫與程序，執行災害預防、緊急應變計畫、復原計畫等防護措施，定期演練以建立應變能量。
2. 對於組織則應規劃建置資通安全整體防護環境，保障機敏資料、文件和檔案存放位置、儲存方式，以及實體隔離等措施。
3. 組織現有網路防護環境，可透過定期弱點掃描，即時修補防護脆弱點。
4. 定期進行安全稽核，強化網路及人員管理機制，期能降低安全威脅及災害損失。

二、事中緊急應變：若不幸遭受入侵或攻擊時，應啟動緊急應變計畫，儘速降低事件造成的損害。

1. 啟動訂定之緊急應變計畫，實施對應之應變處置，並持續監控與追蹤管制，防範事件的影響擴大。
2. 對每起資安事件，應就其發生原因、影響等級、影響範圍、造成損失、支援申請等項目逐一檢討，保留遭受入侵與破壞的相關證據。
3. 透過國家資通安全通報應變網站、弱點(病毒)資料庫或廠商，尋求事件之解決方案；若仍無法順利解決，應請求提供相關技術支援。
4. 視資安事件損壞程度啟動備援計畫、異地備援或備援中心等應變措施，避免事件擴大。
5. 評估資安事件對業務運作造成之衝擊，並進行損害管制。
6. 資安事件如涉及刑責，應做好證據保全工作，並聯繫檢警調單位協助偵查。

三、事後復原作業：檢討現有防護措施，執行復原重建工作，並適時修正現有安全機制漏洞與應變計畫。

1. 執行復原重建工作時，應執行環境重建、系統復原及掃描作業，待系統正常運作後即進行安全備份、資料復原等相關事宜。
2. 完成復原重建工作後，應將復原過程完整紀錄並建檔管制(如資安事件原因分析及檢討改善方案等)，以利往後查考使用。
3. 全面檢討現有網路安全防護，並修補安全漏洞、修正防火牆設定等，避免往後再次遭受類似入侵或攻擊情形，同時視情況修正現有的應變計畫。
4. 資安事件結束後，應彙整事件處理過程紀錄、解決方案及強化措施，提送組織內之資通安全處理小組進行檢討，俾利強化安全防護機制。

肆、結語

資安防護並非一蹴可及，唯有透過完善的安全防護計畫，搭配熟練的緊急應變程序，才可快速掌握突發的資安事件，並完善處理。對於所遭遇的資安事件，除應快速進行事件通報外，仍須回頭仔細檢討事件發生的成因，修補自身的防護缺憾，同時再次檢視原先訂定的安全防護計畫與緊急應變程序是否需要進行相對應修正，以避免往後再次遭受類似的入侵或攻擊情形。經由持續進行「規劃」、「執行」、「查核」、「行動」循環，才可有效加強安全防護能量。

▲Top

在廚房發現一隻蟑螂，就表示家中可能有上百隻蟑螂。

常見的資安攻擊手法案例介紹

◎劉建良

壹、緒論

當發生資安事件時，往往不僅影響單一對象，可能同時造成多人受到波及。推究資安事件發生原因，亦可能同時存在多種入侵管道。然而，如何經由資安事件發生時的徵兆，仔細推敲背後隱藏的意涵，抽絲剝繭並加以查驗後，找到安全防護上真正的漏洞並加以修補，則是處理資安事件時的重點工作。

貳、案例介紹

「奇怪，怎麼一瀏覽ＯＯ網站，防毒軟體突然就跳出警示視窗來了？我是不是中毒了？」沒錯！你可能真的中毒了！這是近來常常發生的情境。民眾在瀏覽網站時，不知不覺就做了「下載惡意程式」的動作，有時防毒軟體可以偵測到惡意程式而加以阻絕，但你確定防毒軟體可以百分之百偵測到所有的惡意程式嗎？當民眾向身為網站主機管理者的你訴說這情形時，該怎麼辦？這個情境到底是怎麼一回事？以下讓我們分成使用者端與伺服器端電腦來進行簡單的情境解析。

一、使用者端電腦

情境：

使用者在開啟瀏覽器後，會自動下載惡意程式回來安裝，若有裝防毒軟體時，可能會跳出警示訊息。

解析：

依據網路傳輸協定，使用者的瀏覽器若要能呈現網頁內容，須先向網站伺服器主機取得網頁的程式碼（如HTML檔）。在取得網頁程式碼後，使用者的瀏覽器就會進行程式碼解譯的工作，將程式碼轉換為人們看得懂的網頁格式，正確地呈現網頁畫面。

「那為什麼防毒軟體會跳出警示視窗來呢？」會出現這種狀況，可能是因為使用者電腦瀏覽了含惡意程式碼的網頁；當使用者電腦的瀏覽器解譯到惡意程式碼後，就會自動執行惡意程式碼所編寫的惡意行為，包含下載惡意檔案、連結惡意網頁等，還可能進一步竊取個人資料、盜取遊戲帳號。此時如果防毒軟體偵測到下載的惡意程式時，就會跳出警示視窗了。

以圖1中駭客植入惡意程式碼的情境來說，當伺服器主機存有漏洞時，駭客可以透過後門程式或是網頁置換攻擊，將惡意程式碼（假設為下載惡意程式）植入到伺服器主機網頁中。這時若使用者瀏覽具惡意程式碼的網頁後，就會將惡意程式碼下載回使用者端電腦執行，並連結到放置惡意程式的伺服器主機下載惡意程式。

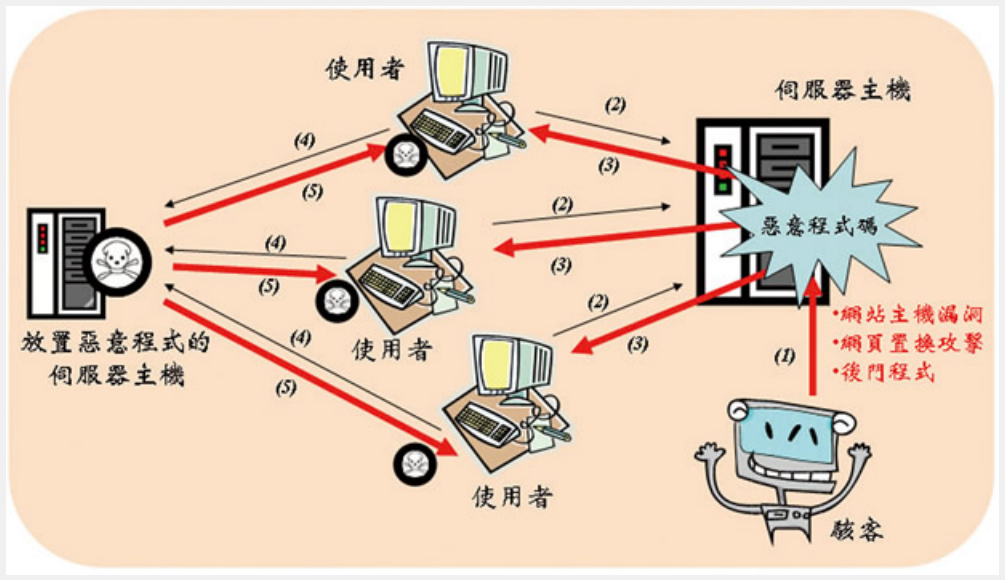

圖1 駭客植入惡意程式碼攻擊情境

二、伺服器端主機

情境：

使用者反應在瀏覽網站頁面後，會跳出防毒軟體警示訊息，懷疑網站伺服器主機已遭受駭客入侵。

解析：

出現此種徵狀時，可能網頁原始碼已遭植入惡意程式碼，使用者端的防毒軟體才會跳出警示訊息。但是否只有網頁原始碼被竄改？還是網站已遭駭客入侵？入侵的程度為何？這些問題，則需做進一步檢測才可得到解答。

「網站主機是不是真的遭駭客入侵？」若這個網站的使用者先前瀏覽行為一切正常，但突然在某一天瀏覽時發生異常時，十之八九是網站遭到駭客入侵。若無法自網站主機找到駭客真正入侵的方式，將無法避免網站再次遭相同手法入侵系統，及植入惡意程式碼。

「駭客是怎麼入侵的？」一般來說，駭客最早入侵一台主機，必須找到一個安全防護漏洞，才能成功取得主機的控制權，通常會透過下列幾種方式：

（一）軟體漏洞：當伺服器主機安裝的作業系統、應用軟體或服務，存在某些未修補的漏洞，而主機管理人員又未進行漏洞更新作業時，駭客即可利用某些手法或工具，侵入伺服器主機。

（二）錯誤設定：主機管理人員對軟體或系統服務項目設定不熟稔，開啟服務項目卻又未限縮使用權限，使得駭客可以正當地取得主機控制權。

（三）系統弱密碼：主機使用的服務項目，或是網站後端系統所使用的密碼強度太薄弱，駭客在猜到密碼後可使用系統提供的功能進行主機控制。

（四）程式開發漏洞：網站程式在開發階段，就具有程式漏洞（如常見的SQL Injection漏洞），駭客透過該程式漏洞可以上傳惡意程式或是執行系統操作等惡意行為。

「駭客發現可以入侵系統時，會做哪些動作？」當駭客可以取得系統控制權時，通常為了可以再次使用系統，最常做的動作是放置後門程式，以便未來可以快速進行遠端指令操作。不過，若軟體無漏洞時，駭客則可能轉而利用程式開發漏洞，竄改網站資料庫內容，這也是最常見的網頁置換、竄改事件。

「後門功能有多強大？」後門程式除了常見的遠端遙控功能外，部分特殊的網頁型後門程式，其功能更是琳瑯滿目，像是基本檔案及目錄操作功能（如新增、修改、刪除等）、CMD指令操作、遠端掃描、服務使用權限提升、批次修改檔案植入惡意連結等（後門程式執行畫面請參照圖2）。基本上只要想像得到的功能，後門幾乎均可做到，而且往往因察覺不易，使得網頁型後門程式存活周期相當的長。

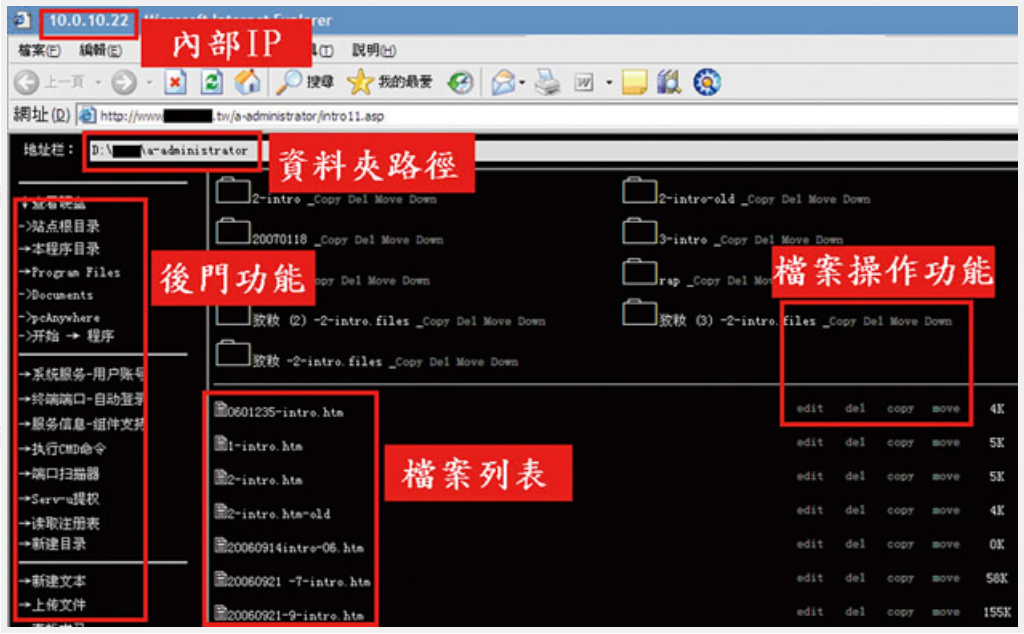

圖2 後門程式執行畫面

「此次案例可能是藉由哪種方式入侵？」當確認主機已遭植入惡意程式碼時，須再檢查惡意程式碼植入位置為何？若惡意程式碼是直接植入於網頁檔案中，則駭客可能是透過後門程式進行檔案修改；若惡意程式碼是植入於資料庫資料中，則可能是透過網站程式開發漏洞（如SQL Injection）進行資料竄改的行為。此外，若是不止一個網頁遭植入惡意程式碼時，則表示駭客可能透過程式或後門，進行大量竄改檔案行為。

「應如何進行安全防護？」若主機曾被駭客入侵，應由發現的入侵徵兆，推敲駭客可能是經由何種途徑入侵主機，並將該漏洞儘速修補完成，避免未來再次遭到相同的手法攻擊。在廚房發現一隻蟑螂，就表示家中可能有上百隻蟑螂；同樣的道理，一旦發現網站主機存有後門程式或漏洞時，主機可能早已淪為駭客的遊樂園，多個駭客族群於主機間已來去自如。因此，資訊從業人員平時就該定期做好系統安全漏洞更新，避免駭客透過未修補的漏洞入侵系統。時時提高警覺，一旦發現有奇怪的跡象時，就該仔細調查主機是否已遭入侵，防患未然。

參、結語

駭客攻擊的手法日新月異，但若仔細推敲其間的變化，可以發現新的攻擊手法多數是藉由前述的各項弱點組合而成，進而影響不同的層級領域。

因此，若要防範遭受資安攻擊，除應做好基本功，補強系統、服務及軟體已知弱點外，在開發網站軟體時亦應注重安全程式碼的概念，避免開發出具漏洞的網頁程式碼。若真的不幸遭受攻擊，也不用灰心，花些心思找出網站弱點進行補強，並澈底清查網站主機，避免後門程式殘留主機內，逐步增強網站安全防護的能量。

（作者是國家資通安全會報技術服務中心經理）

▲Top