網路安全事件應變 Step by Step

運用安全事件應變階段模型 有效防護安全漏洞

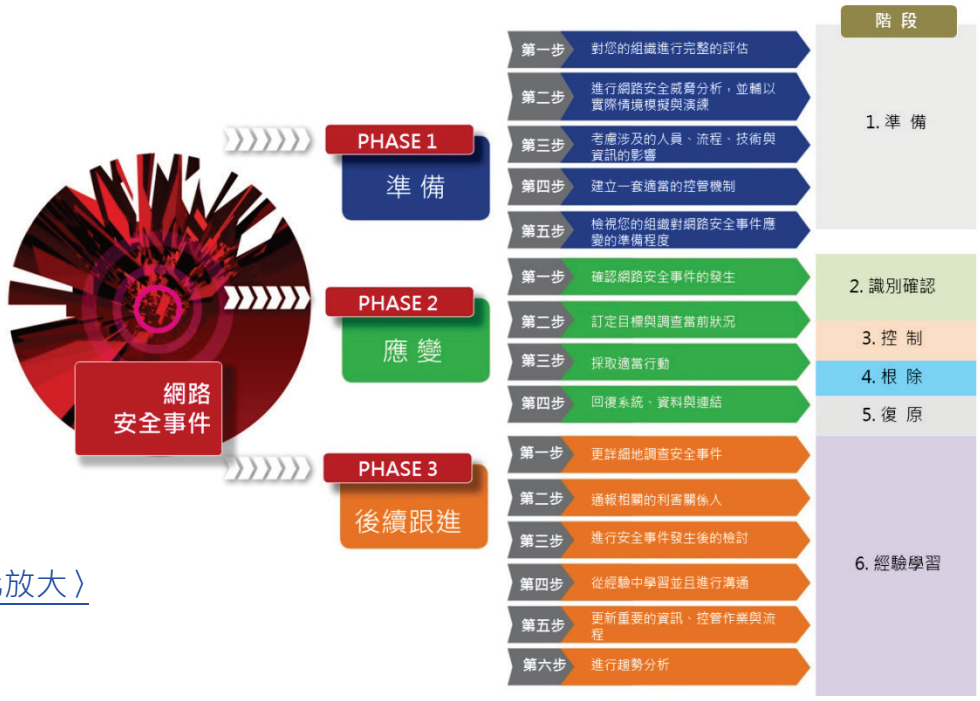
安全事件應變(Incident Response, IR)是指組織運用多種方式為資安漏洞或資料外洩事件做好準備的相關作業。

並非每次的安全事件都是相同的，因此，安全事件的應變人員必須有能力針對不同的狀況做出適當的回應。這需要一個妥善文件化並且易於執行的計畫，讓組織得以迅速根除惡意軟體、勒索軟體或其他類似程式。

本文要探討一個有效的安全事件應變計畫的內容為何，以及要確保成功有哪些重要的關鍵因素絕對不能被忽視。在我們的洞察報告（Insight Paper）《確認網路安全事件應變計畫的有效性》之中，對攸關有效的安全事件應變流程，有全面而詳細的分析。

安全事件應變流程的 6 個階段

非營利組織CREST[1]開發了一個明確的模型，可以分別評估 6 個安全事件應變階段的成熟度。下圖[2]顯示了該模型在安全事件應變流程 6 個階段的管控，以下將逐一詳細分析說明。



〈點此放大〉

[1] CREST 為非營利組織，為提供資訊安全相關服務的個人或公司之品質提供保證。

[2] 原圖來源：http://www.crest-approved.org/cyber-security-incident-response-maturity-assessment/index.html

1 準備 Preparation

在準備階段最重要的是進行安全事件的模擬測試，並做詳盡的分析。這可以讓組織發展出一個詳細的安全事件應變時間表，並將權責分配給最適當的利害關係人。安全事件應變計畫也應該包含對企業擁有的 IR 資源的分析，例如通訊連接埠清單、通訊協定分析、網域架構圖等。經過這些分析，企業將能備妥安全事件應變工具組（IR Tool Kit），準備在安全事件發生時得以應用。

2 識別確認 Identification

組織須確保相關的防禦措施均到位，並能識別出造成影響的指標。確認的項目包含：

- 不尋常的對外網路流量
- 新建立的管理員帳號
- 特許使用者帳戶的異常活動（第一次登入系統）
- 地理區域的不正常行為（非標準模式的登入嘗試）
- 資料庫的存取量大幅增加（轉儲、備份資料庫）
- 大量請求同一檔案
- 可疑的登錄或系統檔案變更
- 非預期的程式修正
- DDoS 活動的跡象

如果資訊安全團隊不認為上述的指標會出現在組織安全系統中，則表示需要更進一步的檢視和分析。

3 控制 Containment

一旦組織確信安全事件可以/將被識別，則接下來重點就會是如何有效控制該安全事件。組織應該依據各種安全事件的潛在影響，訂定出行動方案。IT 或資安權責單位必須檢視是否可以控制各種因素，例如抵禦越權存取、封鎖危險的 IP 與電子郵件地址，甚至網路隔離特定系統等，以此確保相關權責單位擁有完整監控各項可疑活動的能力。

4 根除 Eradication

下一個步驟是排除造成該安全事件的根因（此階段可能與控制階段有所重疊）。這裡的目標是為了消除事件根因、安全事件本身以及影響。一旦完成，最重要的是要確認根除動作已經確實執行完畢，例如監控對外傳輸流量及查看重要的日誌檔。安全事件應變流程須考量以下根除步驟：

- 移除來自網路的攻擊
- 刪除惡意軟體

- 停用被侵入的使用者帳號
- 識別出被利用的脆弱點
- 降低被利用的脆弱點所產生的影響
- 在處理安全事件時，是否有正式的證據處理流程？
- 在處理安全事件時，是否有證據保存的步驟供依循？

5 復原 Restoration

組織必須備妥一份詳細的復原計畫，並確認所有的復原流程都涵蓋在內，以確保能儘速恢復系統功能，例如：用備份檔重置系統、通知相關的利害關係人，及找出網路中類似的弱點等。復原階段也必須確認系統已經全面恢復運作並且受到保護。安全事件應變計畫必須考慮的要素也包括外部滲透測試，以評估復原作業是否夠完備。此外也應該考量提供給利害關係人的資訊的詳細程度以及限期。

6 經驗學習 Lessons Learned

這通常被視為安全事件應變流程中最重要的階段，因為從經驗中學習可以防範未來的安全事件。簡言之，此階段包括：

1. 進行事後檢視，確認在復原過程之中採取的所有行動。
2. 正式紀錄存檔這些事件過程，確認已經學習到哪些經驗，並且將之與相關的利害關係人分享。
3. 更新與修正目前的安全事件應變計畫，以便將這些經驗應用在未來安全事件發生的時候。

結論

即使無法全面為將來未知的安全事件做準備，但是安全事件應變流程裡仍然有些關鍵要素必須要做好準備，以便有效的降低安全事件的後果。最重要的是必須正式定義安全事件應變計畫，並且經常進行評估以確保其效果。運用一個定義明確且有效的安全事件應變架構—一例如 CREST 所發展的安全事件應變流程的 6 個階段—將有助涵蓋安全事件評估作業的各個重要層面。