網絡保安事故應變處理清單

本清單涵蓋事故應變程序及事故處理的必要步驟。

籌備

- **確保系統和應用程式的良好行為**
  - 了解網絡、系統及應用程式的正常行為
  - 識別警報的先兆和跡象
  - 制定日誌保留政策
  - 建立日誌記錄及審計的基線級別
  - 使用及維持正常運作及事故處理步驟的知識庫
  - 保持所有主機時鐘同步
- **加強資料數據保護**
  - 識別和保護敏感資料數據
  - 保護事故中的資料數據
  - 獲取檔案系統備份及系統快照
- **準備事故處理和運作復原計劃**
  - 徵集工具及資源
  - 在事故應變政策中包含報告事故的要求
  - 遵循既定的證據收集和處理程序
  - 建立事故通報機制
  - 保持更新聯絡名單
  - 確保能夠從系統中找出非永久數據作為證據
  - 根據計劃進行事故應變演習
  - 定期檢討和更新計劃

偵測和分析

- **查證事故是否發生**
  - 分析事故先兆和跡象
  - 進行事故關聯分析及研究
  - 記錄調查並收集證據
- **斷定事故處理的優先次序**
- **向適當的內部人員和外部機構通報事故**

遏制、根除和復原

- **收集證據**
  - 獲取、保存、保護及記錄證據
- **遏制事故**
  - 將受影響的主機與網絡隔離
- **根除事故**
  - 識別並緩解被利用的漏洞
  - 刪除惡意軟件、不當材料和其他組件
  - 重複「偵測和分析」步驟以識別所有其他受影響的系統，然後遏制並根除事故
- **從事故中復原**
  - 將受影響的系統復原到運作就緒狀態
  - 確認受影響的系統正常運行
  - 如須要，實行額外的監測措施

事故後的處理

- **撰寫跟進報告，包括事故造成的原因、損失及加強措施**
- **召開汲取經驗會議**
  - 收集不同持份者的意見
  - 議定改進計劃

GovCERT.HK 政府電腦保安事故協調中心

HKCERT 香港電腦保安事故協調中心

香港警務處 Hong Kong Police Force

詳情請在此下載「中小企保安事故應變指南」：