第8章

弱點評估與管理

1. 公開蒐集

多來自媒體，網路社群，公開社群，觀察報告，專業學術活動，深度網路。

1. 蒐集技巧

證書透明度(certificate Transparency，CT);Censys ; 內容安全政策(Content Security Policy ，CSP); WHOIS服務; 自治系統(AS);

1. Google hacking

常用指令:

intext,intitle,cache,define,filetype,info,related,inurl,site;

搜尋引擎 Bing & Shodan;

1. 公共漏洞與暴露

(CVE)Common Vulnerabilities and Exposures 有資安資料庫專門蒐集漏洞

1. 評鑑系統

(CVSS)Common Vulnerability Scoring System

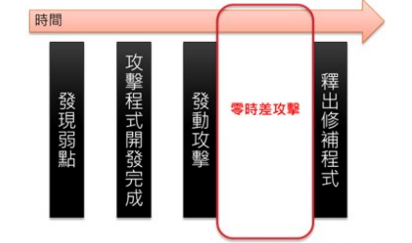
運用數學方程式判定某特定網路是否安全

惡意程式種類與防護

1. 威脅弱點

威脅(threat)弱點(vulnerability):存在的弱點本身不會造成傷害，必須是攻擊才算威脅

1. 零時差攻擊

(Zero-day Attaack 0-day):無法被漏洞工具偵測掃描，並在發布的第一時間攻擊

1. 惡意程式種類

病毒、蠕蟲、木馬程式、釣魚網頁、間諜軟體。

1. 電腦病毒種類/躲避監視種類

複合型病毒(multipartite virus)、巨集病毒(macro virus)、反防毒病毒(retrovirs)、千面人病毒(polymorphic virus)、隱藏型病毒(stealth virus)、變體(metamorphism)、通道(tunneling)、加殼病毒(armored virus)、噬菌病毒(phage virus)、同伴病毒(companion virus)

1. 混和攻擊(blended attack)

電子郵件，視窗的分享資源，網站伺服器，網站客戶端 (IM，P2P)

1. 攻擊工具(特權提升)(Privilege Escalation)

攻擊工具(attacker tools) 後門程式(backdoor) 殭屍程式(zombie)

工具:鍵盤側錄(keylogger) 瀏覽器嵌入軟體(web browser plug-in) 攻擊者工具包(attacker toolkits)

垂直越權提升vs水準越權提升

1. 網際攻擊狙殺鏈(Cyber Kill Chain)

偵查(Reconnaissance)->武裝(Weaponization)->遞送(Delibery)->攻擊(Exploitation)->安裝(Installation)->發令控制(Command and Control C2)->行動(Action on Objectives)

1. 資訊安全防禦機制

制定實施安全政策->資訊安全認證->使用安全防禦工具->正確設定機制

1. 惡意程式事件處理程序

分類(Triage)調查(Investigation)隔離(Containment)分析(Analysis)復原(Recovery)檢討(Review)追蹤(Tracking)

加密勒索軟體攻擊

1. 加密勒索攻擊 (Ransomware)

檔案加密軟體、恐嚇軟體、螢幕綁架軟體。

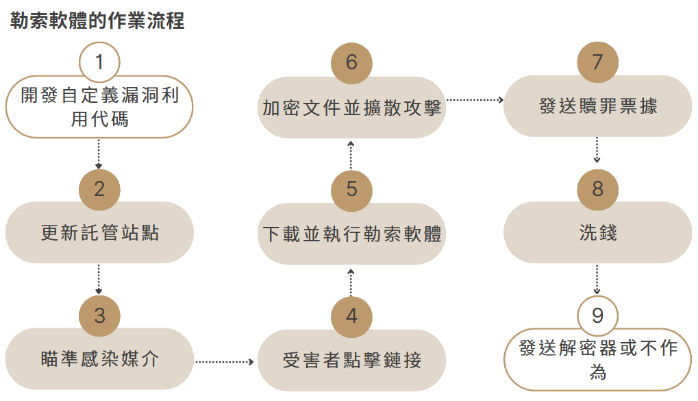
1. 勒索軟體感染方式

主要是攻擊系統的Server Message Block(SMB)服務漏洞。

透過社交工程誘騙使用者，如:抽獎郵件，帳單通知等。

勒索軟體在執行時，會跳出視窗要求匯入指定金額來解鎖。

1. 勒索軟共犯及作業流程



1. 常用技術手法

Spread & Pay Technics(支付技術)

Encrypt & Mining Technics(加密挖礦技術)

File-less Technics(OS白名單技術)

Service Control Technics(服務管控技術)

Bypass Technics(穿透略過技術)

Boot Technics(開機啟動技術)

DLL Hijacking Technics(DLL注入)

1. 感染勒索後的應變措施
2. 斷開網路連接
3. 重製密碼
4. 清除並重新安裝作業系統
5. 確認備份檔案是否含有病毒
6. 確認網路是否安全並下載作業系統及防毒軟體並執行
7. 透過網路資源解密被勒索的檔案。例:no more ransom project
8. 尋求資安專業單位協助處理
9. 藉由TWCERT/CC分享，防範勒索軟體持續猖狂

駭客攻防

1. 駭客分類

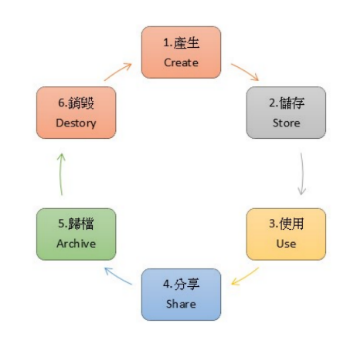
黑帽、白帽、灰帽

1. 階段過程

階段一:決定目標 階段二:蒐集資訊 階段三:發動攻擊 階段四:處理善後

1. 隊伍

白隊、紅隊、黃隊、藍隊、紫隊、綠隊、橙隊。

資訊安全備份管理

1. 生命週期
2. 備援及層次應用
3. 備份
4. 目的 : 通常是複製資料的靜態副本
5. 層次應用 : 資料備份、遠端及時備份
6. 備援
7. 目的 : 資料、軟體與硬體設施的完整複製。動態的救治措施，系統仍在運行狀態下維護運作
8. 層次應用 : 磁碟陣列容錯、被援伺服器、被援服務、異地備援
9. 備份策略

3-2-1原則 :

1. 至少備份三份
2. 使用兩種形式
3. 其中一份備份異地存放
4. 備份計畫內容

決定備份策略需考慮的七點評估要素:

資料的區分、備份方式與媒體、備份位置、備份模式 、備份工具 、備份回復測試

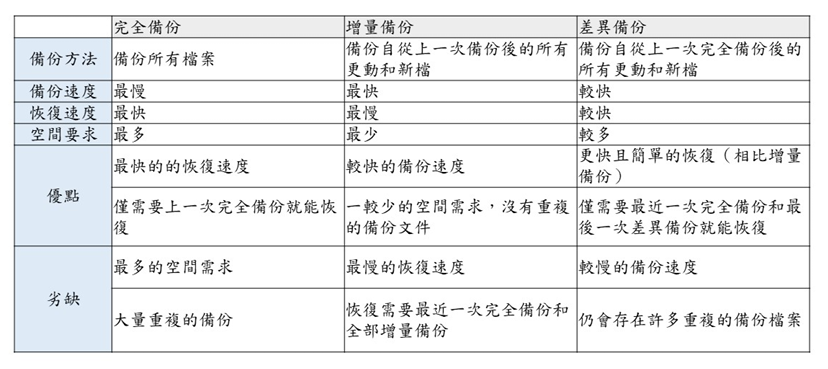
1. 方式與媒體
2. 線上備份(On-line Backup) : 用於需要及時還原的資料
3. 離線備份(Off-line Backup) : 使用可離線的媒體來備份
4. 位置

本機備份、異機備份、異地備份

根據我國電腦機房異地備援機制參考指引，台灣異地備援需再30公里以外，國外一般則在30英哩以外

1. 常見模式

完整備份 ( Full Backup ) 、增量備份 ( Incremental Backup ) 、差異備份 ( Differential Backup )

1. 差異比較
2. 平率與保留週期

根據資料的更新頻率與復原點目標 (RPO)考量

1. 工具

常見硬體 : 磁帶、光碟/藍光CD 、US、外接式行動硬碟、網路儲存設備NAS

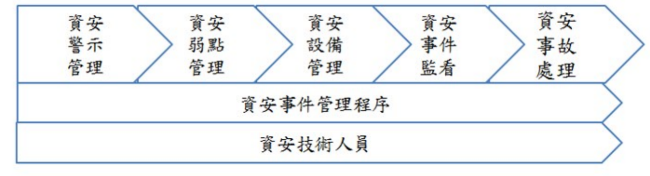
1. 備份回復測試

回復測試紀錄主要記載 : 備份回復日期、回復項目、資料備份日期、備份編號、執行人員、測試狀況、備註以及主管審核項目

日誌管理

1. 資訊安全監控維運中心 ( Information security operation center；SOC )

建置重點在於主動化、自動化、智能化

1. 主要功能
2. 建立基礎 : 人員、管理程序 、相關資訊技術
3. 目的 : 偵測、遏阻、矯治、復原
4. 對資安事件之管理 : 正確辨識、分析、通報、對治行動、調查研究及記錄
5. 五項主要功能 :
6. 八大習慣
7. 習慣1 - 使用自動化的用戶日誌管理工具
8. 習慣2 - 集中收集日誌數據
9. 習慣3 - 保持審計狀態-準備就緒的安全報表
10. 習慣4 - 執行日誌取證調查
11. 習慣5 - 主動應對安全威脅
12. 習慣6 - 跟蹤用戶活動
13. 習慣7 - 數據歸檔和保證日誌數據安全
14. 習慣8 - 持續監控和回顧日誌
15. 安全性資訊與事件管理 ( Security information and event management；SIEM)

功能與一般日誌管理工具類似，都會將來自不同伺服器和設備的日誌和事件紀錄集中在同一個地方。

1. 異常行為
2. 系統中的異常行為 : 程序與服務、檔案、網路使用量、排程工作、帳號、日誌檔內容、其他不尋常的事件。
3. 其他協助工具 :
4. 入侵偵測與防禦系統 (IDS/IPS) : Snort, Suricata
5. 檔案完整性監控 : Tripwire
6. 主機防火牆 : iptables, ufw
7. 安全漏洞掃描 : OpenVAS, Nessus
8. 防毒軟體 : ClamAV