114年三小時以上之一般資通安全教育訓練

**物聯網安全概論試卷(113) 解答**

1. 物聯網的四項挑戰不包含？

答案: 物聯網安全責任歸屬是廠商單方面的責任

1. 許多物聯網裝置使用者介面和雲端應用程式均採用網頁式的介面，請問下列何者並無法有效地降低網頁應用弱點被利用攻擊的風險？

答案:啟用代理連線紀錄

1. 下述何者為物聯網使用者安全性實務建議？

答案:以上皆是

1. 下述何者為常見的物聯網攻擊手法？

答案:以上皆是

1. 目前的物聯網裝置難以實作複雜的安全性機制(例如加密)，其主要原因受限於下列哪一項因素？

答案:記憶容量和運算能力不足

1. 比爾蓋茲在那一年提出「智慧家居」，成為物聯網發展起源。

答案:1995年

1. 以下關於政府機關整體安全管理建議，何者錯誤？

答案:全權交給委外廠商處理

1. 物聯網雖然促進了人類生活上的便捷和各種商機，卻也可能產生嚴重的資安風險， 下列何者是物聯網可能導致的風險威脅？

答案:以上皆是

1. 生活上常見的物聯網應用涉及哪些領域？

答案:以上皆是

1. 物聯網的五種特性，下列何者不是？

答案:規模小

**日常網路使用者應注意的資訊安全 解答**

|  |  |  |
| --- | --- | --- |
| roddayeye整理，嚴禁抄襲 roddayeye.pixnet.net/blog | | |
| Q | r | 由該國家立法規定，其國家範圍的軟體與服務，需要將蒐集到的公民資料，繳交予該國政府控制管理。是下列哪個國家？ |
|  | o | 台灣 |
|  | d | 日本 |
|  | d | 德國 |
| v | a | 中國 |
|  | y | r.o.d.d.a.y.e.y.e. |
| Q | e | 針對資訊安全，安裝軟體更新套件程式（HotFixed Update）可以解決下列哪個資安成因項目？ |
| v | y | 程式設計人員在撰寫程式碼時，產生程式碼的漏洞 |
|  | e | 設定系統設備的相關資料，某些設定項目（config）有疏失 |
|  | . | 電腦與網通設備的使用者有不當行為，致使攻擊者有可乘之機會 |
|  | r | 員工提供的憑證照片不符合規定，導致網路攻擊者藉此入侵系統 |
|  | o | r.o.d.d.a.y.e.y.e. |
| Q | d | 下列何者「不是」資訊安全的防護方式？ |
|  | d | 安裝防毒軟體 |
|  | a | 安裝正版軟體 |
| v | y | 進行1-3-5資料備份 |
|  | e | 更新程式與系統 |
|  | y | r.o.d.d.a.y.e.y.e. |
| Q | e | 在網路社交工程攻擊，針對主管、主管助理與特定人士的攻擊，是何種網路攻擊？ |
|  | . | 垃圾式攻擊（Baiting Spam Mail Attack） |
| v | r | 魚叉式攻擊（Spear Phishing Attack） |
|  | o | 水坑式攻擊（Watering Hole Attack） |
|  | d | 海龜式攻擊(Sea ?Turtle Attack) |
|  | d | r.o.d.d.a.y.e.y.e. |
| Q | a | 關於加密勒索攻擊，下列敘述何者正確？ |
| v | y | 加密勒索的攻擊對象，多半為政府機構、大型企業、醫院學校 |
|  | e | 加密勒索的攻擊過程，在竊密與加密的時候，會產生巨大的網路流量 |
|  | y | 可以透過定期到 Have I been Pwned 網站，降低被加密勒索攻擊的風險 |
|  | e | 透過安裝防毒軟體，可以防範（防堵）加密勒索攻擊 |
|  | . | r.o.d.d.a.y.e.y.e. |
| Q | r | 下列哪個項目是常見智慧行動裝置可能的應用程式（APP）資安問題？ |
| v | o | 安裝APP時，出現異常過多的APP權限要求授權 |
|  | d | 安裝美妝美圖APP程式，卻無法執行 |
|  | d | 安裝行動支付APP需輸入個人資料 |
|  | a | 安裝雲端APP服務，卻無法連線 |
|  | y | r.o.d.d.a.y.e.y.e. |
| Q | e | 針對網路社群網站，下列哪種項目可以瞭解自身帳號密碼外洩的情況？ |
| v | y | 定期到 Have I been Pwned 網站檢查帳號密碼外洩 |
|  | e | 每週檢視（瀏覽）3-2-1檔案備份是否異常 |
|  | . | 每週檢視（瀏覽）YouTube資安教學影片 |
|  | r | 每日檢視（瀏覽）資安新聞網站 |
|  | o | r.o.d.d.a.y.e.y.e. |
| Q | d | 在颱風期間或是連續假期，接獲手機簡訊或電郵通知，要補繳交自來水費用或交通裁罰費用，對於網路社交工程攻擊，這可能是下列哪種攻擊？ |
|  | d | 垃圾式攻擊（Baiting Spam Mail Attack） |
| v | a | 釣魚式攻擊（Web/Email Phishing Attack） |
|  | y | 水坑式攻擊（Watering Hole Attack） |
|  | e | 海龜式攻擊(Sea ?Turtle Attack) |
|  | y | r.o.d.d.a.y.e.y.e. |
| Q | e | 下列哪個項目，「不是」造成資訊安全攻擊的基本形成原因？ |
|  | . | 程式設計人員在撰寫程式碼時，產生程式碼的漏洞 |
|  | r | 設定系統設備的相關資料，某些設定項目（config）有疏失 |
|  | o | 電腦與網通設備的使用者有不當行為，致使攻擊者有可乘之機會 |
| v | d | 員工提供的憑證照片不符合規定，導致網路攻擊者藉此入侵系統 |
|  | d | r.o.d.d.a.y.e.y.e. |
| Q | a | 使用AI網路服務的時候，就資安觀點，下列何者敘述正確？ |
| v | y | 韓國三星公司，使用AI服務的時候，誤將內部機密敏感資料，傳給ChatGPT網路服務，造成資料外洩 |
|  | e | 美國OpenAI公司，疑似遭受駭客DDoS攻擊，導致機敏資料外洩 |
|  | y | 台灣AI廠商，使用中國大陸AI訓練資料， 導致大量敏感個資外洩予中國大陸 |
|  | e | 使用AI服務，可能會造成大量失業，目前不宜貿然學習與使用 |
|  | . | r.o.d.d.a.y.e.y.e. |
| Q | r | 根據2024年9月份，某機構網路服務廠商提供的網路設備與網路服務，當月的可用率已達99%。這表示下列何者項目？ |
|  | o | 當月網路斷網（或停止服務）70小時左右 |
| v | d | 當月網路斷網（或停止服務）7小時左右 |
|  | d | 當月網路斷網（或停止服務）0.7小時左右 |
|  | a | 當月網路斷網（或停止服務）7分鐘左右 |
|  | y | r.o.d.d.a.y.e.y.e. |
| Q | e | 若有公文，受文者為某機構員工，而公文機密等級為"普通"，下列選項何者正確？ |
|  | y | 公文機密等級為普通，表示這份公文可以在新聞媒體公開 |
|  | e | 受文者為某機構員工，表示僅限於該機構記者會可以公布內容 |
| v | . | 受文者為某機構員工，表示公文內容閱讀人員僅限於該機構員工 |
|  | r | 公文機密等級為普通，表示這份公文在新聞媒體僅限於書面閱覽 |
|  | o | r.o.d.d.a.y.e.y.e. |
| Q | d | 關於加密勒索的攻擊步驟，下列敘述何者錯誤？ |
|  | d | 利用社交工程攻擊或設備漏洞，潛入被害人電腦或主機 |
|  | a | 進入被害人電腦主機負責下載進階攻擊程式，並取得帳密，提升權限 |
|  | y | 竊取（搬運）被害人檔案，嘗試網路橫向擴散 |
| v | e | 將被害人個資公布於新聞網站，與被害人進行比特幣贖金談判 |
|  | y | r.o.d.d.a.y.e.y.e. |
| Q | e | 目前已知案例來看，下列敘述何者錯誤？ |
|  | . | 即使是網路實體隔離環境，仍然可能讓攻擊者侵入內部系統。Stuxnet攻擊案例就是其中之一 |
|  | r | 即使是用戶端電腦登入的使用者帳號，仍然可能外洩管理者帳號密碼。Mimikatz就是可以獲取LSASS.EXE的歷史登入帳密工具之一 |
| v | o | 既使是物聯網設備符合國際規範，仍然需要連接AD服務主機控管，進而讓物聯網設備癱瘓。UPnP/SSDP網路攻擊就是案例之一 |
|  | d | 既使是軟體供應商，已經通過ISMS與ISO27001，仍然可能在功英商被入侵後，導致下游克乎端全部被駭客入侵。UNC2452事件（SolarWinds事件），就是其中案例之一 |
|  | d | r.o.d.d.a.y.e.y.e. |
| Q | a | 請問資訊安全的基本觀念"CIA"當中，C這個項目，代表下列哪個項目？ |
|  | y | Continually |
| v | e | Confidentiality |
|  | y | Constantly |
|  | e | Confidently |
|  | . | r.o.d.d.a.y.e.y.e. |
| Q | r | 請問資訊安全的基本觀念"CIA"當中，I這個項目，代表下列哪個項目？ |
|  | o | 保密性（或稱機密性） |
| v | d | 完整性（或稱 一致性） |
|  | d | 可用性（或稱可用率） |
|  | a | 安全性（或稱資安性） |
|  | y | r.o.d.d.a.y.e.y.e. |
| Q | e | 下列何者「不是」常見網路社交工程（Social Engineering）的攻擊手法？ |
|  | y | 垃圾式攻擊（Baiting Spam Mail Attack） |
|  | e | 魚叉式攻擊（Spear Phishing Attack） |
|  | . | 水坑式攻擊（Watering Hole Attack） |
| v | r | 海龜式攻擊(Sea ?Turtle Attack) |
|  | o | r.o.d.d.a.y.e.y.e. |
| Q | d | 針對手機安全防護方式，下列哪種情況可能會被植入惡意程式？ |
|  | d | 手機接獲簡訊，顯示地震通報的假新聞 |
| v | a | 瀏覽網站時，被要求下載更新APP套件 |
|  | y | 接獲電子郵件通知，要求更新銀行帳號密碼 |
|  | e | 開啟電子郵件社交工程測試郵件 |
|  | y | r.o.d.d.a.y.e.y.e. |
| Q | e | 在遇到加密勒索攻擊的時候，可以參考其中的過往解密工具程式，是下列哪個網站？ |
| v | . | https://www.nomoreransom.org/ |
|  | r | https://haveibeenpwned.com/ |
|  | o | https://www.virustotal.com/ |
|  | d | https://www.google.com |
|  | d | r.o.d.d.a.y.e.y.e. |
| Q | a | 關於手機程式的使用權限，下列何者正確？ |
|  | y | 多數人使用的手機APP可以授予較多權限 |
|  | e | 美國歐洲比較重視個資保護，歐美相關手機APP可以授予較多權限 |
|  | y | 開發商信用與商譽評價較高（較好）手機APP可以授予較多權限 |
| v | e | 不要從非官方的APP市場下載APP程式，也不要解除APP權限管制功能（JB越獄） |
|  | . | r.o.d.d.a.y.e.y.e. |
| Q | r | 針對因應加密勒索攻擊的3-2-1檔案備份方式。下列敘述何者正確？ |
|  | o | 3代表是每個月要進行檔案備份三次 |
|  | d | 3表示每週三要進行檔案備份 |
| v | d | 3表示日常工作檔案，需要備份成為3份 |
|  | a | 這表示可能是加密勒索的網路加密活動 |