香港紅卍字會大埔卍慈中學

高中應用學習課程-資訊科技精要

（2023-2025ECC學年）

單元四：數據分析與數據庫

課業四：數據分析書面報告

第一組組員 ：

5D張文桔(組長）

5D黃港寧

5D王偉昌

5A侯柏亨

1. 保護措施

針對惡意軟件攻擊,網絡釣魚,DDoS,網絡入侵,內部人員威脅時,可使用一些保護措施或防禦策略

- 入侵防禦:
  部署入侵偵測和防禦系統,持續監控網絡活動。
  實施嚴格的身份驗證和訪問控制機制。
  定期備份關鍵數據,以便在發生事故時能夠恢復。
- DDoS 防護:
  採用雲端 DDoS 緩解服務或使用專門的 DDoS 緩解設備。
  設定網路路由器和防火牆以阻擋可疑流量。
  與互聯網服務提供商合作,以識別和緩解 DDoS 攻擊。
- 網絡釣魚防護:
  提高員工的網絡安全意識和識別釣魚郵件的能力。
  部署電子郵件篩選系統,阻擋可疑的釣魚郵件。
  建立嚴格的帳號管理和權限控制政策。

有效性和實施成本:

- 入侵防禦:
  組織需要根據自身的網絡規模、安全需求和預算進行成本效益分析。
  可以採取分階段部署的方式,先針對關鍵系統和數據進行保護。
  結合其他防護措施,如身份管理、加密和備份等,形成多重防線。
  定期評估系統性能和有效性,根據需求調整部署方案。
- DDoS 防護:
  組織需要根據自身的網絡規模、業務性質和可承受的風險程度來選擇DDoS防護方案。
  若面臨高頻率或大流量的DDoS攻擊,使用專業服務可能更合適和高效。
  對於低頻或小流量的攻擊,自建系統可能更經濟實惠。
  可以採取混合防禦策略,將雲端服務和本地防護系統相結合。
  定期評估DDoS防護系統的性能和效果,根據實際需求調整部署。
- 網絡釣魚防護:
  組織需要根據自身的業務性質、數據敏感性和風險承受能力來制定最合適的防護策略。
  可以採用分層防護的方式,將重點放在關鍵系統和數據上。
  定期評估防護效果,持續優化和調整部署,提高整體的安全性。
  同時加強員工安全意識培訓,減少員工成為攻擊目標的可能性。

2. OSI 模型連繫:

OSI模型是描述網絡通信的一個標準參考模型,其模型分為七層:

1.物理層:負責定義物理連接設備之間的機械、電氣、功能和過程特性。例如,定義電纜的物理特性、信號的電壓、電流等。

2.數據鏈路層:負責可靠地傳輸數據幀,確保數據在物理層無差錯傳輸。例如,MAC地址管理、差錯檢測糾正等。

3.網路層:負責為數據包選擇最佳路徑,實現端到端的邏輯寄址和路由選擇。最著名的就是IP層。

4.傳輸層:負責在端節點之間提供可靠的數據傳輸服務。最著名的是TCP和UDP協議。

5.會話層:負責建立、維護和同步通信雙方的對話,例如建立驗證的會話。

6.表示層:負責定義數據的語法和語義,確保不同系統之間的數據可以正確解釋。例如,數據壓縮、加密等。

7.應用層:為最終用戶提供網絡服務,例如電子郵件、文件傳輸等。

而物聯網在物理層,網絡層和應用層中經常受到攻擊。舉個例子:

物理層:設備安裝位置不當,容易被惡意物理接觸或破壞,缺乏防護措施,易受到電磁干擾,導致通信中斷。

網絡層:采用IPv4/IPv6協議,存在眾多安全漏洞,易被利用發動DoS攻擊。防火牆配置不當,可能遭受非法訪問和入侵。

應用層:應用程序本身存在漏洞,可能被利用發動遠程控制、信息泄露等攻擊。缺乏良好的身份驗證和訪問控制機制。

3 TCP/IP 模型連繫

物聯網的安全問題主要集中在TCP/IP模型的應用層上。因為物聯網設備大多位於應用層,其內置的軟體、韌體以及應用程式容易存在安全漏洞,使得整個物聯網系統容易受到攻擊因此我們需要透過加密和常更改密碼來解決問題。

主要的安全考慮包括:

1.身份驗證和授權

實施嚴格的身份認證和權限管理,避免未經授權的訪問。例如在智能家居系統中,通過用戶賬號密碼、生物特徵等方式讓用戶身份驗證,並根據賬號權限控制用戶對家電、安防設備等的訪問權限。

2.加密和安全通信

對通信內容和傳輸過程進行加密,確保數據的機密性和完整性。
例如在車聯網系統中,對車輛傳感器採集的行車數據進行加密處理,並採用安全的通信協議如TLS/SSL進行加密傳輸,防止數據被攔截和竄改。

3.固件/軟體更新機制

例如在工業設備監控系統中,定期自動檢查並更新設備的軟體固件版本,修補已知的安全漏洞,保證設備始終運行在安全狀態。

3.4 網絡架構模型連繫

物聯網的安全問題可以與零信任網絡架構模型相關聯。零信任網絡模型是一種用於保護機構的安全性模型，其依據為不應預設信任任何使用者或裝置，即使對方已存在於機構的網路內。零信任機制會在整個網路上 (而不只是在信任的範圍內) 強制執行嚴格的身分驗證和授權從而保護物聯網的隱私上問題。

在物聯網的情境中，零信任網絡架構的應用意味著：

1. 身分驗證:要求進行嚴格的驗證和授權,確認來源、合法和目的等。需要確保安全性和不可否認性非常吻合。強調不信任任何實體,必須對每個參與者進行嚴格驗證,包括使用數位證書、生物識別等技術。

2. 密碼學技術應用:使用密碼學技術,如數位簽章,確保完整性和防篡改,對於安全性至關重要。要求對所有網絡流量進行持續監控和分析發現異常行為,可幫助發現異常、惡意攻擊等情況,配合機器學習等技術,可建立更智能異常檢測和預警機制,加密技術使用可防未經授權訪問,進一步增強安全性。