中小企業網絡安全的七大攻略

安全層面	控制理念	最佳實踐	自我評估（✓所適用的）
1. 安全政策和安全管理	安全政策是企業裡的重要文檔。 它闡明了管理層在網絡安全風險管理方面的安全要求和態度。管理層應建立一種機制，定期維護和宣傳安全政策對員工的要求。	✓ 員工應有機會閱讀安全政策，了解公司的安全要求，並在入職時確認他們會遵從要求。 ✓ 安政策應放在員工可以輕易參閱的地方。 ✓ 安全政策應定期更新，也應讓員工定期重新確認政策。	☐ 我的機構沒有安全政策 ☐ 我的機構有安全政策，員工可以輕易參閱安全策略 ☐ 員工入職時需要確認安全政策 ☐ 員工需要定期重新確認安全政策

2. 端點安全	端點是指員工在工作期間存取業務訊息時使用的個人電腦或筆記本電腦。電子郵件通信，網頁瀏覽和其他業務應用程序都在端點上運行。攻擊者希望入侵端點，因為它可以用作存取企業有價值訊息資產的入口點。	✓ 端點電腦應受到防病毒和反惡意軟件等安全軟件的保護。 ✓ 病毒特徵檔和安全軟件應保持最新，以保護端點免受最新威脅。 ✓ 端點電腦操作系統的安全補丁也應保持最新。 ✓ IT 人員也應監控端點的更新狀況。 ✓ 端點上的用戶帳戶應該是普通非特權用戶（非管理員） ✓ 瀏覽網頁時應使用代理伺服器過濾惡意超鏈結	☐ 我的機構沒有安裝任何端點保護軟件 ☐ 我的機構已安裝端點保護軟件，但不知道病毒特徵檔是否是最新的 ☐ 我的機構安裝了端點保護軟件，並定期更新病毒特徵檔 ☐ IT 人員定期檢查端點保護軟件的更新狀態 ☐ 端點電腦操作系統的安全修補程序並不會定期更新 ☐ 端點電腦操作系統的安全補丁會定期更新 ☐ 用戶在端點上使用的帳戶是非特權的 ☐ 已設置代理伺服器在瀏覽網頁時過濾惡意超鏈結

3. 網絡安全	大多數企業都利用互聯網促進商業訊息交換。互聯網的連接帶來了外部攻擊者可能從外部侵入企業網絡的網絡安全風險。企業應正確配置防火牆，設定好面向互聯網的伺服器和其他網絡設備，以避免入侵。	✓ 應正確配置防火牆，盡可能減少企業暴露於互聯網的網絡端口。 ✓ 防火牆上的默認規則應為“DENY”。僅根據業務需求“允許”某些網絡流量 ✓ 不允許所有內部網絡的設備存取互聯網。僅允許部份已轄准的 IP 地址存取互聯網。 ✓ 不允許從互聯網到內部伺服器的遠程訪問（例如 RDP） ✓ 應定期審查防火牆規則	☐ 我的機構沒有使用防火牆來保護公司網絡 ☐ 我的機構有使用防火牆來保護公司網絡 ☐ 防火牆上使用默認“DENY”的規則 ☐ 防火牆不允許所有內部網絡設備存取互聯網 ☐ 防火牆不允許遠程訪問 ☐ 有定期審查防火牆規則

4. 系統安全	企業利用訊息系統來處理業務資訊。一些系統（例如，網頁伺服器）對互聯網開放以發放或收集訊息。這些系統是攻擊者的目標，因為系統包含有價值的的訊息。企業應為執行關鍵任務的系統制定系統安全準則和指引。	✓ 應設置密碼政策，使伺服器密碼滿足最小長度和復雜性要求 ✓ 伺服器應強化安全設定，啟用安全政策並禁用不使用的服務 ✓ 應及時更新系統補丁以防止最新的威脅 ✓ 面向互聯網的伺服器應避免存儲敏感訊息。在伺服器中儲存敏感資料時，應把敏感資料屏蔽或加密 ✓ 應用程序接收來自互聯網用戶輸入的資訊時（例如 Web 服務器表單），應正確過濾輸入，以避免 SQL 注入類型的攻擊 ✓ 對於服務公眾及執行關鍵任務的系統，應由專業人員定期進行滲透測試	☐ 我的機構有伺服器密碼政策，密碼需要滿足最小長度和複雜性要求 ☐ 我的機構有強化系統安全設定及禁用未使用服務的伺服器安全指引 ☐ 我的機構有定期更新系統補丁的流程 ☐ 面向互聯網的伺服器不儲存敏感訊息 ☐ 儲存敏感訊息時，敏感訊息被屏蔽或加密 ☐ 應用程序有過濾用戶輸入，以避免 SQL 注入類型的攻擊 ☐ 專業人員定期對關鍵任務系統進行滲透測試

5. 安全監控	由於無法 100%確保端點，服務器和網絡的安全性，企業應建立機制來監控和檢測訊息系統中是否發生可疑事件。越早確定威脅，可以越早採取行動，可以最小化威脅帶來的潛在損害	✓ 應在網絡設備（例如防火牆）和伺服器中啟用日誌記錄 ✓ 日誌記錄應集中儲存在某個位置，方便進行定期審查和監控 ✓ 應及時檢查日誌記錄，以便正確處理檢測到的問題 ✓ 應監控網絡流量（例如互聯網流量），以檢測流量模式是否有任何突然變化	☐ 我的機構防火牆和伺服器都啟用了日誌記錄 ☐ 日誌記錄集中收集在日誌伺服器中 ☐ IT 人員定期審查日誌 ☐ 當系統檢測到異常時，設置有自動機制通知 IT 人員 ☐ 網絡流量模式包含在監控中

6. 事件處理	因系統問題或安全事件導致系統中斷是不可能百份百避免的。企業應針對不同類型的事件製定應對計劃，包括惡意軟件感染等小事件，以至需要系統恢復的重大事件。	✓ 根據不同的情況制定事件應對計劃（包括不同類型的安全事件） ✓ 定期備份系統和數據，並且離線儲存（甚至異地儲存） ✓ 演練恢復程序以確保可以正確恢復備份	☐ 我的機構沒有任何事件應對計劃 ☐ 我的機構有處理不同類型事件的事件應對計劃 ☐ 我的機構有系統和數據的備份計劃 ☐ 備份數據保持離線狀態 ☐ 定期對恢復計劃進行演練，以確保備份可以恢復

7. 用戶意識	用戶是網絡安全中最薄弱的環節。95%的安全事故涉及人為因素。企業應確保員工了解他們在保護企業訊息資產方面的角色和責任。	✓ 應定期提醒員工保護機構訊息資產的角色和責任，例如：員工意識培訓 ✓ 可以執行演習（例如模擬網絡釣魚攻擊）來測試員工是否準備好應對常見的網絡攻擊	☐ 我的機構沒有任何對員工的安全意識活動 ☐ 我的機構有為員工提供定期的安全意識培訓 ☐ 我的機構有執行模擬測試，以評估員工對常見網絡攻擊的準備情況

自我評估分數計算

得分 ＝ 藍格✓數目 － 黃格✓數目

33 至 26： 保安十分充足
25 至 18： 保安充足
19 至 10： 保安須加強
11 至 3： 保安鬆懈
2 至-5： 保安十分鬆懈