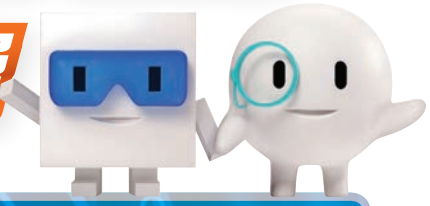
資料來源：香港生產力促進局和香港電腦保安事故協調中心

# 中小企網絡安全七大攻略 應對網絡保安威脅



**在智能科技普及應用的年代，企業高度依賴資訊系統協助日常營運，若不做好資訊保安工作，就有機會令業務癱瘓，甚至洩漏客戶私隱資料，影響企業形象。香港生產力促進局早前發表的「 SSH 香港企業網絡保安準備指數調查 」顯示，「 中小型企業 」的網絡保安準備指數僅得 43.4 分，大多未有定期評估保安風險，改善保安設備和管理質素。為此，該局及屬下香港電腦保安事故協調中心編制《中小企網絡安全七大攻略》，從七個層面分享良好作業模式，以及自我保安風險評估的步驟，協助中小企應付日趨複雜的網絡保安威脅。**

香港生產力促進局於 2018 年 4 月發表「 SSH 香港企業網絡保安準備指數調查 」，顯示「 中小型企業 」的網絡保安準備指數只得 43.4 分，未達 60 分或以上的理想門檻。為協助長期資源緊絀的中小企，該局及屬下香港電腦保安事故協調中心編制《中小企網絡安全七大攻略》，從資訊保安政策和資訊保安管理、端點保安、網絡保安、系統保安、保安監察、保安事故處理及用戶意識七個層面作出分析。

## 資訊保安政策和資訊保安管理

在資訊保安系統中，制定正確的資訊保安政策，管理員工妥善地執行政策是重中之重，是決定保安水平的關鍵要素。有關的資訊保安政策由管理層策劃，須因應本身的營商環境和資源，並配合業務需要和風險管理策略而制定。資訊保安政策是一個機構實現保安目標的基本指引和途徑，但絕非是一成不變，機構可根據實際情況及資訊保安要求的變化，適時更新資訊保安政策。

管理層制定政策之後，需要在機構上下推廣和落實，並監察政策的執行情況。推行資訊保安政策有三大方法：

1. 各位員工（尤其新員工）應有機會查閱及知悉資訊保安政策，了解企業的資訊保安要求，並在工作中積極遵守。
2. 資訊保安政策應張貼在當眼處，以及在公司內聯網上發佈，方便員工查閱。
3. 資訊保安政策應定期更新，並確保員工知悉，例如即時向員工發送電郵介紹新政策，更新辦公室的海報及公司內聯網的文件。

資訊保安政策的制定與管理是一個持續的過程，需要管理層及企業上下員工的通力合作，才能確保資訊保安政策妥善執行。

## 端點保安

在資訊泛濫的年代，電腦是工作上不可或缺的好助手。與此同時，網絡安全事件也無日無之，因此企業也可從端點保安著手，加強防護。

### 何謂「端點」？

企業員工在日常業務中所使用的電腦或設備，只要連接網絡，便可界定為「端點」。最常用的電子郵件通訊、瀏覽網頁或使用商業應用程式，也在端點上進行。所以，端點就是網絡的門戶，駭客一般會從較易存取、保安較差的端點來入侵企業的網絡系統。保護端點就等於守護網絡系統、防止駭客入侵的第一道防線。以下六招，可加強端點的保安防護：

1. 所有端點電腦應安裝防毒及防惡意程式軟件；
2. 網絡保安軟件的病毒資料庫及主程式，應保持最新版本及定期更新；
3. 端點電腦應適時安裝修補程式，以堵塞系統漏洞；
4. 電腦部門員工應監察用戶電腦的更新情況；
5. 用戶帳號只應設有最低限度的合適權限，並與擁有管理員權限的帳號分開使用；
6. 瀏覽網頁時，使用代理伺服器阻擋可疑網址。

在「自攜裝置」(BYOD) 的趨勢下，部份企業亦會准許員工使用自己的手提電話或平板電腦，進行公司的商業活動和通訊，以提升工作效率。企業應建議員工提高網絡保安意識，包括：

1. Android 操作系統應安裝可靠的防毒軟件。
2. 切勿破解手機的保安設定（「越獄」Jailbreak）或獲取根權限（Root）。
3. 切勿安裝或下載任何不知名或不可信的應用程式。
4. 切勿瀏覽任何可疑網頁。

## 網絡保安

由於資源有限，不少中小企未能有效地保護網絡，成為網絡攻擊的受害者，嚴重者更可能洩漏企業敏感資料，後果不可小覷。若企業能根據網絡保安的最佳實務指引來配置網絡，並定期評估網絡保安水平，便可大幅減低受網絡攻擊的風險。以下是四招網絡保安貼士：

1. **使用防火牆**：使用防火牆保護企業的網絡服務，把公眾可以存取的服務與內部網絡分開，例如使用防火牆分隔，把公司網頁伺服器及數據庫伺服器分開兩個網絡。
2. **限制遠端連接企業網絡**：必須妥善管理遠端存取企業網絡，確保於安全的情況下才啟用，例如使用虛擬私有網路 (VPN) 或雙重認證 (Two Factors Authentication)，避免成為駭客入侵企業網絡的入口，切忌貪圖一時之便，讓資訊科技支援公司長期啟用不安全的遠端存取。
3. **限制企業內電腦連接互聯網**：互聯網並非百分之百安全，其實企業內並非所有電腦都要連接互聯網，尤其是金融機構員工的電腦。因此，企業可以考慮只容許有需要的電腦連接互聯網，以降低風險，以避免因開啟不明超連結 (URL) 而感染勒索軟件。

4. **定期評估企業網絡保安水平**：企業應定期進行專業的網絡保安水平評估，以避免發生網絡事故，並減少因事故所造成的經濟損失，同時又影響商譽。

## 系統保安

網絡之外，載滿財務或敏感資料的企業電腦系統也是駭客虎視眈眈的目標。對中小企而言，系統保安對防止資料外洩及保持資料完整極為重要。為方便工作，現時很多內部伺服器都可透過遠端服務來存取。然而，一些中小企曾因系統的重要檔案被勒索軟件加密而嚴重影響運作，並向香港電腦保安事故協調中心求助。這類事故的起因，往往是遠端伺服器保安出現漏洞或設定不足所致。

最基本的保護措施，是採取安全有效的密碼政策。其次，還要留意伺服器的設定是否妥當，並及時更新與修補程式。若機構提供對外的網上服務，則必須留意網站保安。提到網站保安，企業一般只會留意防火牆或 HTTPS 加密協定，卻忽略了網站應用程式設計，而最常見的情況是並無檢查用戶所輸入的數據，因此導致網站被插入惡意程式碼，繼而洩露網站資料庫的所有資料。

另外，對於敏感資料，機構應留意分類及保密措施，例如為資料設定不同的保密程度，並把敏感資料加密。這樣的話，即使資料外洩，駭客也難以解密，無法得到資料詳情，從而減低對企業的影響。

系統維護也是保安的重要一環，卻經常被人們忽略。許多企業只重視購置防火牆或防毒軟件等防禦措施，卻忽略了定期更新系統的保安設施。現有系統或網站在操作一段時間後，可能會出現各種漏洞，故各企業應定期檢查系統，掌握系統的最新問題，才能及早採取應對措施，堵塞漏洞。

## 保安監察

企業要保護自己公司的電腦系統，維護自身利益責無旁貸，但很難百分百確定端點、伺服器和網絡的安全，因此日常保安監察變得非常重要。企業需要建立一套有效的機制，監控和偵測機構的資訊科技系統有否發生可疑事件。及早發現問題，便可即時採取行動，把潛在的威脅減至最低。

「SSH 香港企業網絡保安準備指數調查」的結果發現，即使香港企業正使用既有的保安方法及技術偵測網絡威脅，惟連基本的門檻都尚未可達。企業若要實行良好的資訊保安監察，可參考以下實踐方法：

- 啟用網絡設備（例如防火牆）和伺服器的日誌記錄功能，以便詳盡記錄公司每位員工使用網絡資源時的連接嘗試及活動等日常作業。
- 把有關記錄儲存於特定的日誌伺服器，方便審查和監察。
- 相關保安人員應定時審核日誌，以便及早發現問題，盡快妥善處理。
- 要定期監察網絡流量（例如互聯網流量），以偵測流量模式是否出現不尋常的變化。

## 保安事故處理

近年，企業頻受電腦保安事故威脅，例如企業資料外洩、遭受勒索軟件攻擊等，情況岌岌可危。對中小企而言，規劃完善的保安事故處理程序是刻不容緩的。企業必須要做好資訊保安防禦工作，並建立危機事故處理程序，以便可以及時處理事故，免招損失。

規劃危機事故處理程序時，企業務必要考慮前、中、後三個階段的應變安排：

- **前期工作**：制定危機事故處理政策。除了把駭客犯罪行為加入處理政策外，還要制定火災、水災等災難應變措施，同時要定期為系統和數據進行遙距離線備份。除此之外，企業要定期測試備份復原系統，以確保備份資料完整無誤；
- **事故發生期間**：即時啟動應變程序。若不幸發生事故，應根據危機事故處理政策的安排，通知相關人員，即時採取應變，務求可以盡快恢復運作；以及
- **後續工作**：檢討及評估。善後工作完成後，應調查及檢討事故發生的原因，評估再次發生事故的風險，同時需要審視現有系統的安全架構及危機事故處理政策，進一步加強安全措施，防患未然。

網絡保安事故不但影響企業運作，更會嚴重打擊公司聲譽，甚至令企業面臨巨額罰款或賠償。規劃完善的事故應變程序，或有助為機構樹立良好的公眾形象。

## 用戶意識

美國權威電腦保安培訓機構 SANS Institute 分析指出，95% 的網絡安全事故皆由人為。用戶稍一不慎下載了可疑郵件中的惡意檔案，便可能引發安全事故。為了防患於未然，企業應向員工灌輸最新的網絡安全意識，確保員工了解自身對保護信息資產 (Information Assets) 的責任。若用戶能成為守護網絡的最後一道防線，定能減低發生網絡保安事故的風險。

香港電腦保安事故協調中心建議企業定期為員工提供培訓，認識最新的網絡安全事故趨勢，加以學習和提防。現今數碼發展蓬勃，釣魚網站肆虐，企業務必要提醒員工妥善管理電郵，尤其應該即時刪除可疑電郵，還要教導員工如何分辨勒索電郵的真偽。

早前有用戶收到色情網站的勒索電郵，聲稱其電腦透過網站感染了惡意軟件，被內置攝錄鏡頭拍下了用戶的不雅照片，藉以勒索金錢。電郵上甚至披露了受害人的賬戶名稱和密碼，受害人誤信被要脅便繳付贖金。然而，用戶的電腦事實上未必真正被入侵，不法分子可能根本沒有植入惡意軟件，更沒有拍下任何畫面。

除了培訓之外，企業亦應定期進行網絡安全事故演習，測試員工是否充分準備應對常見的網絡攻擊，例如發出模擬的詐騙或勒索電郵，並附有可疑檔案，測試員工會否「中招」，以及有多少員工會主動舉報，藉以提升員工辨別及舉報可疑電郵的意識。

## 總結

《中小企網絡安全七大攻略》根據七個層面，剖析中小企能如何從不同方面加強保安防護，以及採取良好作業模式。此外，香港電腦保安事故協調中心的網頁上，載有列明保安風險自我評估清單的指引，以應對層出不窮的網絡保安威脅，詳情請瀏覽：www.hkcert.org/my_url/zh/guideline/18091101 ■