標準網路防護

電腦網路不斷受到攻擊。不過，只有少數攻擊成功。大部分的網路攻擊是伺機性的，並不是針對特定的受害者，而只是刺探性質，例如，掃描開放的網路/連接埠、嘗試容易猜到的密碼、找出未修補的網路服務或傳送網路釣魚電子郵件。攻擊者不想花費任何時間或精力進行失敗的攻擊，所以他們只會轉移到下一個可能的受害者。

如果您認為這相當於一個在路上閒逛的偷車賊試著拉動門把，直到他找到一輛未鎖的車子為止，那麼同樣地，只要遵循一些標準的網路強化建議 (亦即，離開前不要忘記鎖車門)，就可以保護自己免受伺機型攻擊！使用內建防火牆的路由器、在電腦上使用難以猜測的密碼，以及將您的作業系統和軟體維持在最新狀態是您在家就可以做的簡單事情。在過去 10-20 年灌輸我們的觀念包括：不要開啟來自未知寄件者的附件；安裝反惡意軟體；不要從不受信任的網站安裝軟體，以及不要插入您剛才在路上發現的 USB 隨身碟 。

但這是 Axis 的部落格，那麼 網路攝影機如何？安裝時有什麼風險 (如果有的話)？幸好攝影機不會受到與電腦相同的威脅。攝影機不需要使用者登入、安裝軟體、造訪網頁或開啟電子郵件附件。不過，攝影機所提供的服務可能會讓攻擊者想要當做其他攻擊的平台使用。「物聯網」遽增導致許多上網裝置 (包括攝影機) 不夠堅固，這些裝置很容易就會成為駭客們在殭屍網路中「奴役」的目標。

因此，這裡有一些簡單的建議，可以減輕來自伺機型攻擊者的風險：

減少網路曝露

基本上，除非真的需要，否則不要將任何裝置連線至網際網路。如果這麼做了，則請務必了解，在進行該步驟之前，裝置必須夠堅固，才能連線至網際網路。

網路攝影機的挑戰在於許多人希望能夠從遠端存取影像。網路攝影機包含一部網頁伺服器，您通常只要使用網頁瀏覽器，就可以存取影像。在路由器/防火牆中戳一個洞 (稱為連接埠轉發)，並使用網頁瀏覽器做為主要的影像用戶端似乎是一個好主意，但這會增加不必要的風險，因此我們不建議採用。

基於開放的優勢，我們應該注意到 Axis 攝影機一直以來都支援 UPnP NAT 周遊，這是一種簡化路由器連接埠轉發設定過程的服務。

但是，預設不會啟用而且我們也不建議啟用此服務。這是舊版功能，之後的產品將會移除此功能。現在有更好更多的方式可以從遠端存取影像。對於沒有 VMS (影像管理系統) 的個人和小型組織，Axis 建議使用免費的 AXIS Companion 用戶端，此用戶端不需要將攝影機 (以裝置的方式) 曝露在網際網路之下，就可以從遠端安全地存取影像。對於使用 VMS 的系統，我們則建議您遵循 VMS 廠商對於遠端影像存取的建議進行。如果您的影像串流處理至公開位置 (例如網站)，則建議您使用媒體 Proxy 搭配設定正確的網際網路網頁伺服器。此外，如果您有多個遠端站點，則最好使用 VPN (虛擬私人網路)。

難以猜測的密碼

幾乎與其他所有支援網際網路的裝置一樣，密碼是攝影機的主要防護，以防止未經授權者存取其資料和服務。關於強式密碼的定義有很多爭論。其中一個常見的建議是使用最少 8 個字元，並混合大/小寫字母、數字和特殊字元。對於強式密碼而言，暴力密碼破解登入攻擊並不實用，因為這可能需要花數千年的時間。在 VMS 環境下，驗證主要是機器對機器，因為使用者無法直接存取攝影機。在 VMS 環境下增加登入失敗延遲可能會提高鎖住自己的方顯。在較小的組織中，用戶端通常會直接連線至攝影機 (人機驗證)，因此建議您使用難以猜測但容易記住的密碼。使用冗長的複雜密碼做為密碼，例如「this is my camera passphrase」。是的，允許使用空格。但是，無論您怎麼做，請不要直接使用出廠預設密碼。

韌體和軟體修補

軟體是由人類所製造，而且人類仍然容易犯錯 (到目前為止)。因此，即使我們在軟體上市之前已經盡最大的努力抓出漏洞，定期還是會發現漏洞，而且會一直持續下去。大部分的漏洞並不嚴重但有些漏洞可能是嚴重的，因此，請務必將您的韌體和軟體維持在最新狀態，並定期檢查新的版本。發現嚴重漏洞時，假設在經濟上是可行的，就是某些人利用這個漏洞的大好時機。如果攻擊者可以存取未修補的網路服務，則他們非常可能會成功，這就是為什麼減少這些機會非常重要的原因之一。

針對性攻擊

企業和重要基礎架構組織不僅容易受到伺機性攻擊，也容易受到針對性攻擊。這些攻擊將會使用與以往相同的低成本媒介，但是針對性攻擊者有更多時間、資源和決心，因為在危急關頭有更多價值。為確定應該使用哪些安全控制來降低您的風險，進行威脅建立模式與風險分析相當重要。這是一個很大的主題，我將在之後的部落格文章中詳細說明。

Axis 職責

我們一直致力於降低客戶的風險，包括改善我們的開發流程和產品生命週期、提供更好的安全控制、更安全的預設設定、加強使用者介面以及其他指導方針，例如這篇部落格文章。如果您想要深入了解如何以更妥善的方式加強網路攝影機，請閱讀本指南以獲得更多建議。