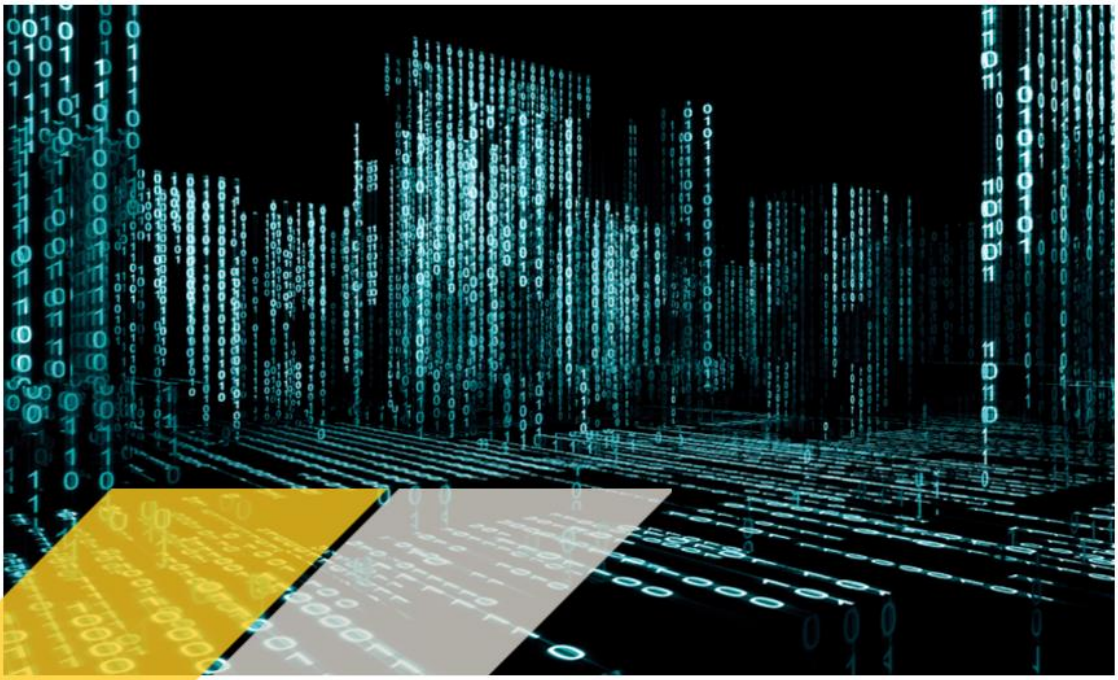

網路攝影機 – 不要讓您的網路門戶洞開

雖然互聯網的願景吸引了大量連線裝置網路提供的便利性、功能和靈活度，但隨著網路進入點的數量急劇增加，安全性威脅和入侵行為的風險也不斷增長。在 Cisco 最近的一項調查中，73% 的企業決策者表示，他們預計在未來兩年內，物聯網將導致安全性威脅的嚴重性增加。更令人擔憂的是，78% 的 IT 安全專業人員對其功能不確定，或者認為他們缺乏保護新型網路連線裝置安全所需的能見度和管理能力。

隨著網路存取越來越容易，隨之而來的入侵風險也就日益增加。設計系統時，應該將周密的系統威脅/風險分析納入考量。如同您新增至系統的任何應用程式般，攻擊暴露面積將會隨著新元件的加入而增加。加入影像系統將會增加暴露面積，就像是在所有電腦上安裝 Microsoft Office 套件會增加額外的網路風險一樣。影像系統元件可能會對其他網路資源增加風險，同樣地，在網路上加入額外的資源也會對影像系統引進風險。將攻擊面積減至最小是一種常見的網路防護措施。**如果裝置、服務和應用程式不需要互動，則您應該嘗試限制彼此之間的連線。**隔離影像系統與其餘的網路是一個很好的整體防護措施，可降低影像資源和業務資源以負面或危險的方式彼此影響的風險。

與網路上其他裝置 (例如筆記型電腦、桌上型電腦或行動裝置) 不同的是，網路攝影機不會曝露在使用者造訪可能有害的網站、開啟惡意的電子郵件附件，或安裝不受信任的應用程式等常見威脅之下。不過，攝影機或其他連線的實體安全性裝置是具有介面的網路裝置，可能會曝露風險。因此，減少這些威脅的曝露面積相當重要。

保護或加強影像安全系統安全的程序是安裝人員和 IT 人員越來越需要了解的程序。一份好的的強化指南可提供適合特定使用者需求的設定策略，以處理不斷演變的威脅情勢。Axis 使用 SANS Top 20 Critical Security Controls 做為其強化指南的基準。第一步是了解並使用業界標準的安全通訊協定，包括多層使用者驗證/授權、密碼保護、SSL/TLS 加密、802.1X、IP 過濾和憑證管理。

此外，攝影機供應商 (如 Axis) 還會透過新功能、錯誤修正和安全性修補程式不斷更新其攝影機韌體。為因應日益增長的風險、安全風險的種類和數量，安全系統使用者需要隨時掌握其供應商的最新狀態，並留意透過網路攝影機系統預防攻擊的最佳做法。