

智能樓宇互聯

資料安全性



資料安全性

確保實體層資料安全

駭客從不挑剔，他們會利用任何設備以任何訪問級別潛入。如您所知，結果可能是災難性的。根據 Ponemon Institute 在 2018 年 7 月公佈的一項研究報告，企業網路資料洩露的平均成本高達 386 萬美元。此外，在遭到駭客攻擊後，24 個月內再次受到攻擊的可能性為 27.9%。經濟損失僅僅是一個開始。在遭到駭客攻擊後，企業可能需要數年時間才能重新獲得信任並重建其聲譽。

在當今的超連接智慧樓宇中，每個網路連接都是進入網路的一扇門。為了避免未經授權的訪問，您需要為每一層網路加鎖並保護每個入口點 - 從應用級別的加密到身份驗證、虛擬私人網路 (VPN)、防火牆到最終的實體層安全性。正如網路中的每個元件一樣，實體層基礎設施是為了防止入侵或其他最壞情況而進行正確規劃的關鍵部分。

COMMScope®

在 2015 年發生的所有資料安全性漏洞事件中，有 **60%** 源于內部人員的有意或無意行為。

2015 年網路安全情報指數，IBM Security

網路基礎設施已經成為一個容易受到攻擊的目標

長久以來，安全性是在較高的網路邏輯層實現的。隨著商業樓宇網路的發展，企業在各個方面的集成度越來越高，這使得實體層成為容易受到攻擊的目標。誰控制了網路路由基礎設施，就等同於誰控制了流經網路的資料。在醫療保健和金融等行業，網路安全問題催生了有關資料存儲的新法規和合規性要求。網路基礎設施安全問題通常分為兩類：

27%

人為錯誤

系統故障

25%

48%

有意犯罪攻擊

2018數據洩露成本研究，Ponemon Institute

- **未經授權人員進行未經授權的訪問**可以通過部署與 IP 相連的攝像頭、在場感測器、存取控制和所連接的其他物理安全性群組件來減少或預防。可以通過部署物理佈線安全裝置（如鍵控連接器、安全跳線和埠阻止器）來降低未經授權訪問所帶來的威脅。類似的是，自動化基礎設施管理 (AIM) 解決方案可以記錄和報告實體層上任何未經授權的活動。
- **獲得授權人員進行未經授權的訪問**可能更難檢測和阻止，這是由於物理的安全性群組件可能無效造成的。在這些情況下，AIM 解決方案可以自動記錄和報告所連接的任何非授權網路設備（包括其物理位置），並跟蹤實體層的任何即時變更。



實施建議

正確的連接策略可以在很大程度上保護您的資料免受本機攻擊。需要考慮的重點事項如下：

實體層監控和檢測

自動化基礎設施管理 (AIM) 系統能夠即時監控和報告實體層中所有獲得授權和未經授權的變更。通過使用智慧佈線、連接器和配線架，這些系統就能自動記錄所有變更並提醒管理人員注意新的和不定期的連接，例如希望插入筆記型電腦以獲得未經授權訪問的入侵者。此外，AIM 系統也可以與現有的入侵偵測系統集成，以識別入侵的確切位置並將此資訊傳送給入侵偵測系統。一些 AIM 系統，如康普的 imVision® 也可以與企業的防毒軟體集成，通過物理位置識別惡意或受感染的設備，最大限度地降低攻擊造成的損失和損害。



康普 imVision Controller X
讓整個連接環境一目了然

室內無線系統

隨著駭客不斷發現新的漏洞，一度被認為是安全的安保措施也在被惡意利用。其中一個例子就是 Wi-Fi 系統使用的 WPA2 安全協定。利用用戶端和 WPA2 接入點之間交換時存在的弱點，入侵者就能突破加密連接。在蜂窩或移動網路中，安全設置由服務提供者集中管理。這些安全措施必然比傳統的企業 Wi-Fi 系統更加強大、靈敏。

安全監控和感測器

通過增強型連接（如智慧樓宇中的連接）可以實現由 IP 安防攝像頭和在場感測器組成的網路，從而說明發現未經授權的入侵者。借助適當的綜合佈線基礎設施，就可以將這些乙太網供電 (PoE) 設備放在所需的各個位置，從而實現優化覆蓋。

光電混合纜/PoE佈線

在光電混合纜或乙太網供電網路中，所有連接的設備都從交換機獲取電力，而交換機通常由 UPS 電池和發電機供電。這種集中式的供電結構本身更易恢復運行，也更安全。即使主電源發生故障，AIM 系統和所有連接的安保設備都將繼續運行。

Powered fiber cable system



與康普攜手合作， 充分挖掘企業網路的應用潛力

隨著企業網路互聯性的不斷提高，保護敏感性資料變得更具挑戰性。防範風險是一項值得大力投入的工作。沒有人比康普更瞭解您的商業樓宇網路基礎設施。

40 多年來，康普一直代表著安全保障和促進商業樓宇網路創新的推動力。我們不斷參與制定行業標準和開發相關實踐，擁有充分的願景和經驗，足以幫助您創建更智慧、更高效的工作空間。您清楚自己的需求 - 我們知道下一步該怎麼做。讓我們攜手發揮您的潛力。



COMMScope®

commscope.com

請造訪我們的網站或聯絡當地的 CommScope 代表人員，取得詳細資訊。

© 2018 CommScope, Inc. 保留所有權利。

除非另有說明，帶有 ® 或 ™ 的所有商標皆分別為 CommScope, Inc. 的註冊商標。本文件僅供規劃階段使用，非用於修改或增補 CommScope 產品或服務的任何相關規格或保固。CommScope 致力於達成最高標準的業務完整性與環境永續性，位在世界各地的眾多服務設施已取得 ISO 9001、TL 9000 和 ISO 14001 等國際標準認證。關於 CommScope 承諾的其他深入資訊，請造訪 www.commscope.com/About-Us/Corporate-Responsibility-and-Sustainability。

MC-113149-ZHTW_SECURITY