白皮書

網路安全

基本概念與專業用語

AXIS COMMUNICATIONS

目錄

1. 簡介

本文件的目標對象是想要瞭解網路安全基礎的個人和組織，透過簡要的敘述、模式和結構概述網路安全概念和專業用語，並聚焦於實體安全系統。本文件可作為其他安迅士網路安全相關文件的專業用語和定義參考資料。

2. 網路安全

網路安全的定義有很多種。維基百科的描述是指電腦安全：

> *電腦安全又稱為網路安全或資訊科技安全，是避免電腦系統的硬體、軟體或資訊遭竊或受損，以及防止提供的服務中斷或遭到不當使用的保護機制。*

要保護您自身的上網安全，不能只靠單一防護措施。數位安全與您使用的工具無關；而是與您對所面臨威脅的瞭解以及如何應對這些威脅有關。為了提升安全，您必須決定您要保護的資產以及要防範的對象。威脅可能依您所在的環境、從事的工作及合作的夥伴而異。因此，為了找出最適合您的解決方案，請您進行威脅模式評估。

3. 風險評估

在網路空間中進行風險分析的過程類似實體保護的風險分析。在實體世界，通常需要保護的對象是實體物品、建築物和人。在網路空間中，資訊/資料相當於資產，服務相當於資源。實體侵害比較容易被察覺，竊盜和損壞也更明顯。

進行風險評估時的五個基本問題：

1. 您想要保護什麼？
2. 您想要防範的對象是誰？
3. 您需要防範對方的可能性有多高？
4. 若未做好保護，後果可能有多嚴重？
5. 為了嘗試防止這些後果，您願意付出多少努力？

ISO 27000 資訊保護標準攸關於資產機密性、可用性和完整性 (又稱為資訊安全三要素)。

如果您無法存取您的資料或使用服務、資料損壞或資料外洩給未經授權者，會產生什麼影響？為了評估影響，必須將資料分類，因為不同類型的資料可能具有不同的價值。

ISO 將資料和服務分成限制、私人或公共。舉例來說，影像系統可能會依以下方式分類影像系統資源：

> 即時影像歸為公共類別，公共可能指一般大眾或組織內的群眾。如果即時影像曝光於公眾，造成的傷害相對有限。

> 錄影可能歸為私人類別，只能由特定組織單位存取，因為某些錄影事件可能具敏感性。

> 系統設定、帳戶和密碼歸為限制類別，只有組織內的特定人士可存取。

4. 威脅概況

駭客利用安全漏洞攻擊系統的背後一定有潛在原因。攻擊可分為伺機性或針對性。在網路安全領域中，攻擊者又稱為惡意或無意 (或意外) 對資產造成傷害的對手。

現今絕大多數攻擊屬於伺機攻擊，也就是趁機攻擊。在許多情況下，伺機攻擊者不知道受害者是誰。這些攻擊者採用低成本的攻擊向量，例如掃描開放的網路、服務和連接埠、嘗試預設或常用密碼、尋找未修補的服務以及發送釣魚郵件。伺機攻擊者不會將時間或資源耗費在一次失敗的攻擊上，如果失敗，他們將尋找下一個受害者。採用標準保護等級將降低多數伺機攻擊相關的風險。

相較之下，鎖定特定系統且具有特定目的的針對性攻擊較難防範。針對性攻擊採用與伺機性攻擊相同的低成本攻擊向量。然而，如果首次攻擊失敗，針對性攻擊者會依目標價值繼續嘗試，並且願意花費時間和資源採取更複雜的方法。針對性攻擊者常利用複雜的社交工程和魚叉式網路釣魚 (針對特定接收者精心製作的電子郵件) 來存取系統。如果失敗，他們會分析系統、軟體或流程以找到替代安全漏洞。

5. 威脅者及其動機

透過瞭解誰是最有可能的攻擊者，您可以深入瞭解其可能的動機、願意花費的時間、資源和精力，以及可能針對的安全漏洞。

> 親友：想要窺探您私生活的人。

> 員工，或具有合法存取權限的人員：無意或蓄意濫用職權者。

> 惡作劇者：以干擾電腦系統為樂者。

> 激進駭客：以政治或意識形態為動機攻擊組織者。

> 網路罪犯：有意透過詐欺或出賣有價值的資訊牟利者。

> 同業：想為所屬公司爭取利益者。

> 網路恐怖主義者：嘗試藉由攻擊發出警告或引起恐慌，達到意識形態或政治目的者。

> 國家 (外國情報機構)：想要獲得經濟/政治利益或對重要資訊系統造成損害者。

> 個人：獨立行動的特定人士或團體，其動機可能與上述不同，例如調查記者或白帽駭客。如果您將資源用於隱藏缺陷和安全漏洞，而不是進行修復，則白帽駭客 (道德駭客) 可能會構成威脅。

6. 攻擊價值和成本

攻擊價值取決於相對於攻擊成本、侵入得手能帶來的利益。網路安全的目標是使攻擊的成本大於利益，從而降低攻擊價值 (價值=利益 — 成本)。為了採用適當的保護等級 (建立攻擊成本)，必須瞭解可能的威脅。雖然每個系統都可能遭受到任何威脅者基於任何意圖的攻擊，但某些威脅比其他威脅更有可能發生。瞭解較可能發生的威脅有助於識別安全措施的重點 (哪些安全漏洞可能被利用)。

7. 常見的組織類型和威脅

攻擊的負面影響通常取決於受害者的組織類型。

組織類型	範例	可能的攻擊者	影響
小型組織	> 消費者 > 家庭企業 > 非營利組織	> 親友 > 惡作劇者 > 伺機性駭客	個人等級 > 隱私權 > 完整性
企業組織	> 產業 > 公司 > 零售商	以上項目加上： > 員工 > 激進駭客 > 犯罪組織 > 同業	企業等級 > 金錢損失 > 停機 > 信任 > 智慧財產 > 競爭優勢
基礎建設	> 能源/水 > 銀行/金融 > 電信 > 交通運輸 > 公共衛生 > 軍警	以上項目加上： > 國家 > 網路恐怖主義者	公共等級 > 安全 > 供應 > 恐慌

8. 風險

人們對「風險」可能有不同的定義。RFC 2828 網際網路安全詞彙將風險定義為：

預期損失為特定威脅利用特定安全漏洞可能產生的特定損害結果。

在許多情況下採用速記公式：風險 = *概率*影響*。此公式用於對不同類型的威脅排列優先順序。RFC 定義用「特定」一詞描述威脅、安全漏洞和損害結果。應分別檢視各個威脅，從可能性最高且負面影響最大的威脅開始檢視。

針對各種保護類型 (機密性、可用性和完整性)，必須對威脅的負面影響有基本的認識。這項任務很困難：在許多情況下，預估相當主觀，而影響常被低估。ISO 27000 影響類型 (有限、中度嚴重、非常嚴重或災難性) 可幫助您快速概覽以排列優先等級。您可以將影響類型想像成恢復所需的時間，將影響程度換算成：有限=小時/天、中度嚴重=週、非常嚴重=月、災難性=年。

9. 安全控制

新增安全控制的過程稱為強化。安全控制為用於避免、偵測、抵消或最小化實體財產、資訊、電腦系統或其他資產的安全風險之保護措施或對策。補償控制是替代保護措施，當可能無法採用建議的安全控制，或建議的保護措施成本可能太高時，可以採用補償控制。

限制存取和降低曝露會降低系統的可用性。為了在系統可用性和系統保護之間取得平衡，通常需要在系統使用者的需求和安全管理員的需求之間達成折衷的協議。如果過度限制，使用者可能會尋找忽略保護的方法，從而造成新的安全漏洞。可用性和保護之間的期望平衡需要由系統所有者定義。

10. 安全漏洞和風險曝露

安全漏洞為攻擊者提供存取系統的機會，可能造成缺陷、功能或使用者錯誤；攻擊者可試圖利用安全漏洞，通常結合一個或更多個安全漏洞，以達成其最終目的。

研究顯示超過 95% 的侵入得手可歸咎於三個因素：人為錯誤、設定不良的系統及維護不當的系統。它們通常是缺乏適當的規範和定義的責任所導致的結果。

設備 API (應用程式介面) 和軟體服務可能具有可在攻擊中利用的缺陷。沒有廠商能保證產品完美無瑕。如果知道缺陷所在，可以透過補償安全控制來降低風險。反之，如果攻擊者發現未知的缺陷，可能會產生零時差漏洞，不留給受害者任何保護系統的應變時間。

非重大安全漏洞是影響性較低的漏洞，或雖然潛在影響可能很嚴重，但難以被利用的漏洞。利用重大缺陷可能需要符合一些條件，包括連上網路及使用其提供的資源。

常見安全漏洞評分系統 (CVSS) 是一種對軟體安全漏洞的嚴重程度進行分類的方法，藉由公式來查看安全漏洞被利用的簡易度，以及可能產生的負面影響。分數採用 0 到 10 之間的數值，10 代表最嚴重。在已發佈的常見安全漏洞和曝露 (CVE) 報告中常能找到 CVSS 數值。安迅士採用 CVSS 作為評估軟體/產品安全漏洞嚴重程度的方式之一。

曝露在判斷安全漏洞風險中也扮演重要角色。攻擊者能否輕易利用安全漏洞？取決於基礎建設、服務曝露和日常操作。
例如：在企業商業入口網站服務的公共網站伺服器上，安全漏洞的風險可能分類為非常嚴重。而在本機保護網路上的攝影機中使用時，同樣的安全漏洞可能分類為有限。

11. 安全漏洞掃描

安全漏洞掃描是對軟體或產品的自動或手動審查。市面上有幾種此類掃描工具。安全漏洞掃描嘗試識別具有已知安全漏洞的服務。此類服務如果曝露給攻擊者，可能會遭到利用。

安全漏洞掃描只能找出已知的安全漏洞，結果不適合當做衡量產品安全性的標準。明天可能會發現新的重大安全漏洞。安全漏洞掃描有時會與滲透測試混淆。滲透測試是您主動嘗試忽略安全控制，而安全漏洞掃描是只找出潛在的安全漏洞。

12. IP 過濾

IP 過濾如同攝影機的本機防火牆。在專業影像系統中，影像管理系統 (VMS) 是系統的中心。影像用戶端無法直接從攝影機存取影像：即時影像和錄影透過 VMS 服務提供給用戶端。這表示在正常操作期間，VMS 伺服器應該是存取攝影機的唯一電腦/伺服器。如果影像系統位於非影像用戶端可能連上攝影機網路的非隔離網路，可以設定 IP 過濾作為附加保護。透過 IP 過濾，攝影機不會回應未列於白名單中的任何 IP 位址的請求。白名單應包括可用於故障排除和維護的 VMS 伺服器、安迅士攝影機管理系統 (ACM) 伺服器和其他個人電腦 (如果有的話)。

13. 網路隔離 (網路分割)

網路隔離是一種將多個重要的網路資源互相隔離的方法，以便降低其中一個網路資源對另一個網路資源有負面影響的風險。隔離尤其適用於不需要 (或不應該) 互相作用的資源。網路分割可能是虛擬的 (VLAN)，需要配置網管型交換器的基礎建設；網路也能與不同的佈線和網路設備隔離。要採用的分割類型取決於成本、基礎建設和規範。

良好的整體保護是將實體安全網路與其他 (網域) 網路資源隔離。如果一個網路上的影像用戶端需要存取另一個網段上的 VMS 伺服器，可以在兩個網段之間新增防火牆。防火牆只能打開用戶端和 VMS 伺服器之間的流量，而不能打開攝影機的流量。

14. 網路加密 — HTTPS

網路加密可保護用戶端、VMS 和攝影機之間的通訊，防止透過網路流量探查擷取資訊，並防止資料在傳輸過程中遭竄改。網路加密不一定會增加對攝影機、VMS 或用戶端的保護。

安迅士攝影機支援 HTTPS (採用安全 SSL/TLS 通道的 HTTP)。用戶端 (例如 VMS) 也需要支援 HTTPS。HTTPS 將加密所有管理流量 (一般 HTTP 流量)，但不一定會加密影像，因為會透過即時串流協定傳輸。如需加密影像，VMS 必須也支援要求在加密的 TLS 通道上採用即時串流協定。並非所有 VMS 都提供支援，詳情請洽 VMS 廠商。攝影機必須具有憑證 (自行簽署或 CA 簽署)，而且必須設定 HTTPS 規範，才能建立 HTTPS。

15. 憑證授權中心 (CA)

使用自行簽署或 CA 簽署的憑證對於加密等級並沒有不同。差別在於自行簽署的憑證不能防止網路詐騙 (在攻擊性電腦試圖模擬合法用戶端或伺服器的情況)，而 CA 簽署的憑證為用戶端新增信任點，確保存取信任的攝影機。CA 簽署的憑證用於 HTTPS (伺服器憑證) 和 802.1x (用戶端憑證)。

公用與私人 CA

公共信任的 CA，如 Comodo 和 Symantec (舊名為 Verisign) 通常用於公共網站和電子郵件伺服器等公共服務。在多數作業系統 (Windows、Linux、Mac) 和瀏覽器中，預先安裝了用於公共信任 CA 的 CA 根憑證。

私人 CA 是內部/私人網路服務的信任點，也是為所有內部用戶端和伺服器發出憑證的軟體/伺服器 (通常為 Active Directory/憑證服務)。私人 CA 根憑證必須安裝在存取私人資源的所有用戶端中。視可用的工具和基礎建設而定，可以採用手動或自動的方式佈建憑證。

16. 網路存取控制 — 802.1X

IEEE 802.1X 是防止未經授權的網路設備存取本機網路的標準。設備必須通過身分驗證，才能存取網路 (及其資源)。可以採用不同的驗證方法，如 MAC 位址 (MAC 過濾)、使用者/密碼或用戶端憑證。由系統所有者決定採用哪種方法，而適當的選擇依威脅、風險和成本而異。

操作 802.1X 基礎建設是一項投資，需要配置網管型交換器和其他伺服器，通常是 RADIUS (遠端驗證撥號使用者服務)。使用用戶端憑證需要可發出用戶端憑證的 CA (私人或公共)。在多數情況下，基礎建設需要執行維護和監控的人員。如果使用者尚未備妥 802.1X 基礎建設，新增網路影像/安全系統時不會新增此基礎建設。可提供替代措施給 802.1X 的補償控制可作為減少不同重要網路資源曝露的網路隔離方式。

17. SNMP

SNMP (簡易網路管理通訊協定) 用於收集和整理 IP 網路上的網管型設備相關資訊。採用 SNMP 監控攝影機有助於偵測攝影機故障和可能受到攻擊的斷線。

18. Syslog 伺服器

所有攝影機都配備一個記錄攝影機中所有操作的內部日誌。此日誌可能會因攝影機重新開機而遺失，或遭到入侵攻擊者清除或竄改。遠端 Syslog 伺服器可在日常操作期間收集所有攝影機日誌訊息。使用遠端 Syslog 伺服器保護日誌，可簡化故障排除或鑑識調查，以便發現異常情況和入侵跡象。

19. 更多資訊：

www.axis.com/support/product-security

> AXIS 安全漏洞規範

> AXIS 強化指南

> 安全通報 (CVE)

> 白皮書

www.axis.com/learning/online-courses

> AXIS 安迅士學院網路安全訓練

www.axis.com/blog/secure-insights/category/cyber-security

> 關於網路安全的各種主題

71007/TW/R1/1708

關於安迅士

安迅士致力於提供智慧安全監控解決方案，期望使世界變得更智慧、更安全、更有保障。身為網路影像監控市場的領導者，安迅士持續帶領業界推出創新的網路產品，而這些產品全數基於一開放式的技術平台，因此能透過全球合作夥伴網路為客戶創造最高價值。安迅士擁有長遠緊密的合作夥伴關係，並提供夥伴們專業知識與卓越的網路產品，以共同耕耘現有及開創新監控市場領域。

安迅士在全球 50 多個國家擁有超過 2,700 位員工，並提供遍及全球超過 90,000 家合作夥伴的強大支援。安迅士成立於 1984 年，總部位於瑞典，並以 AXIS 名稱於那斯達克斯德哥爾摩證交所掛牌上市。

相關安迅士之更多資訊請參閱本公司網站 www.axis.com

AXIS COMMUNICATIONS