安讯士与网络安全

所有网络设备均受制于网络威胁，包括网络摄像机。网络摄像机往往是大型系统的一部分，而网络则是骨干。不管是作为系统还是作为独立设备，所有部分都很容易受到攻击，需要对整个系统加以保护。

最薄弱的一环决定着企业的强健程度。

安讯士设备能够配置为不同的安全级别。《**安讯士安全强化指南**》现已公布在公司网站上！

能否提供更高级别的网络威胁防护，取决于企业是否拥有 IT 和网络策略及相应的风险分析。基于 IP 的设备可提供额外的价值和智能。通过减少曝光区域和规避风险，我们能够帮助您提高系统安全性。尽管网络攻击无法预防，安讯士漏洞策略（在公司网站上提供）介绍了合作伙伴和用户有望从安讯士获得的收益。

安讯士网络安全使命：
> 提高对安全行业的认知
> 提供思想领导力
> 根据利益相关方的运营情况和需要，帮助他们实现适当级别的摄像机/视频系统保护

www.axis.com/support/product-security

AXIS COMMUNICATIONS

安讯士的十大网络安全建议

1. 对潜在威胁以及如果系统被攻击或破坏可能造成的损害/成本进行风险分析。
2. 了解系统保护情况和可能的威胁。与经销商、系统集成商、顾问和产品供应商密切合作。互联网是一项无与伦比的资源。
3. 保护网络安全。如果网络保护出现缺口，将增加敏感信息被窃和单个服务器及设备遭到攻击的风险。
4. 使用强大、唯一的密码并定期进行更换。
5. 不得依赖于网络设备的出厂默认设置。
   > 更改默认密码。
   > 启用和配置设备保护服务。
   > 禁用未使用的服务。
6. 尽可能使用加密连接，即使在局域网上也是如此。
7. 为了降低曝光风险，除非系统/解决方案需要，否则视频客户端不得直接访问摄像机。客户端应只通过 VMS （视频管理系统） 或媒体代理服务器访问视频。
8. 定期检查访问日志，查看是否有非法访问企图。
9. 定期监控设备。在适用且支持的情况下，启用系统通知。
10. 使用最新的适用固件，因为其中可能包含安全补丁。

www.axis.com/support/product-security

AXIS COMMUNICATIONS