Axis Communications and Cybersecurity

All network devices are subject to threats, including network cameras. A network camera is always part of a larger system where the network is the backbone. All parts are vulnerable, either as a system or as individual devices and the system as a whole needs protection.

You are only as strong as your **weakest link.**

Axis devices have the ability to be configured for different levels of security. The **Axis Hardening Guide** is now published on our website!

Providing a higher level of protection against cyber threats depends on your organization's IT and cyber policies combined with an appropriate risk analysis. IP-based devices provide additional value and intelligence. Together we can make your system more secure by reducing exposure areas and mitigating risks. While attacks cannot be prevented, Axis' Vulnerability Policy (available on our website) describes what partners and end users can expect from Axis.

Axis' cybersecurity mission:

> raise awareness to the security industry
> provide thought leadership
> help stakeholders achieve an acceptable protection level for cameras/ video systems based upon their operations and needs

www.axis.com/support/product-security

AXIS® COMMUNICATIONS

Axis Communications' Top 10 Cybersecurity recommendations

1 Make a risk analysis of potential threats and the possible damage/cost if the system is attacked.

2 Gain knowledge on system protection and possible threats. Work closely with resellers, system integrators, consultants, product vendors. The internet is a fantastic resource.

3 Secure the network. If network protection is breached it increases the risk of snooping for sensitive information and attack individual servers and network devices.

4 Use strong, unique, passwords and change them on a regular basis.

5 Do not rely on a network device's factory default settings
> Change default password.
> Enable and configure device protection services.
> Disable services that are not being used.

6 Use encrypted connections when possible, even on local networks.

7 To reduce exposure video clients should not be allowed to access cameras directly unless it is required by the system/solution. Clients should only access video through a VMS (Video Management System) or a media proxy.

8 Check access logs on a regular basis to detect attempts on unauthorized access.

9 Monitor devices on a regular basis. Enable system notifications when applicable and supported.

10 Use the latest applicable firmware as it may include security patches.

www.axis.com/support/product-security

AXIS® COMMUNICATIONS