Cybersecurity Q&As

User manual

Cybersecurity Q&As

For other questions and answers, visit the Axis *FAQ database*.

Cybersecurity Q&As

General questions

General questions

What is cybersecurity?

Cybersecurity is the protection of computer systems and services from cyberthreats. Cybersecurity practices include processes for preventing damage and restoring computers, electronic communications systems and services, wire and electronic communications, and stored information to ensure their availability, integrity, safety, authenticity, confidentiality, and nonrepudiation.

Cybersecurity is about managing risks over a longer period of time. Risks can never be eliminated, only mitigated.

What is generally involved in managing cybersecurity?

Cybersecurity is about products, people, technology and ongoing processes.

It will, therefore, involve **identifying** and evaluating various aspects of your organization, including doing an inventory of devices, systems, software, and firmware; establishing mission-critical objectives; documenting procedures and security policies; applying a risk-management strategy and continuously performing risk assessments related to your assets.

It will involve implementing security controls and measures to **protect** the data, devices, systems, and facilities that you've identified as priorities against cyber attacks.

It will also involve developing and implementing activities that help you **detect** cyber attacks so you can take timely actions. This could, for instance, involve a Security Information and Event Management (SIEM) system or a Security Orchestration, Automation and Response (SOAR) system that manages data from network devices and management software, aggregates data about abnormal behavior or potential cyber attacks, and analyzes that data to provide real-time alerts. Axis devices support the SYS Logs and Remote SYS Logs that are the primary source of data for your SIEM or SOAR system.

Cybersecurity management also involves developing and implementing procedures to **respond** to a cybersecurity incident once it is detected. You should take into account local regulations and internal policies, as well as requirements for disclosure of cybersecurity incidents. Axis offers an *AXIS OS Forensic Guide* that will help you understand if an Axis device has been compromised during a cybersecurity attack.

Developing and implementing activities to maintain plans for resilience and to **recover** or restore any capabilities or services impaired due to a cybersecurity incident will also be important. *AXIS Device Manager*, for instance, makes it easy to restore Axis devices by supporting restore points, which are saved "snapshots" of system configuration at a point in time. In the absence of a relevant restore point, the tool can help return all devices to their default states and push out saved configuration templates via the network.

What are the cybersecurity risks?

Cybersecurity risks (as defined by RFC 4949 Internet Security Glossary) is *an expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.*

It is important to define clear system policies and processes in order to achieve adequate risk reduction over the long term. A recommended approach is to work according to a well-defined IT protection framework, such as ISO 27001, NIST or similar. While this task may be overwhelming for smaller organizations, having even minimal policy and process documentation is far better than having nothing at all.

For information on how to assess risks and prioritize them, see *Cybersecurity reference guide*.

What are the threats?

A threat can be defined as anything that can compromise or cause harm to your assets or resources. In general, people tend to associate cyber threats with malicious hackers and malware. In reality, negative impact often occurs due to accidents, unintentional misuse or hardware failure. Attacks can be categorized as opportunistic or targeted. The majority of attacks today are opportunistic: attacks that occur just because there is a window of opportunity. Such attacks will use low-cost attack vectors such as phishing and probing. Applying a standard level of protection will mitigate most risks related to opportunistic attacks.

General questions

It is harder to protect against attackers who target a specific system with a specific goal. Targeted attacks use the same low-cost attack vectors as opportunistic attackers. However, if the initial attacks fail, they are more determined and are willing to spend time and resources to use more sophisticated methods to achieve their goals. For them, it is largely about how much value is at stake.

What are the most common threats and how can they be addressed?

Deliberate or accidental misuse of a system

People who have legitimate access to a system is one of the most common threats to any system. They can be accessing services that they are not authorized to. They may steal or cause deliberate harm to the system. People can also make mistakes. In trying to fix things, they may inadvertently reduce system performance. Individuals are also susceptible to social engineering; that is, tricks that make legitimate users give away sensitive information. Individuals may lose or displace critical components (access cards, phones, laptops, documentation, etc). People's computers may be compromised and unintentionally infect a system with malware.

Recommended protections include having a defined user account policy and process, having a sufficient access authentication scheme, having tools to manage user accounts and privileges over time, reducing exposure, and cyber awareness training.

Axis helps counter this threat with *hardening guides*, and tools like *AXIS Device Manager* and *AXIS Device Manager Extend*.

Physical tampering and sabotage

Physically exposed equipment may be tampered with, stolen, disconnected, redirected or cut.

Recommended protections include placing network gear (for example, servers and switches) in locked areas, mounting cameras so they are hard to reach, using protected casing when physically exposed, and protecting cables in in walls or conduits.

Axis helps counter this threat with *protective housing* for devices, tamper-resistant screws, cameras with the ability to encrypt SD cards, detection for camera view tampering, and detection for an open casing.

Exploitation of software vulnerabilities

All software-based products have vulnerabilities (known or unknown) that could be exploited. Most vulnerabilities have a low risk, meaning it's very hard to exploit, or the negative impact is limited. Occasionally, there may be discovered and exploitable vulnerabilities that have a significant negative impact. MITRE hosts a large database of CVE (Common Vulnerabilities & Exposures) to help others mitigate risks.

Recommended protections include having a continuous patching process that helps minimize the number of known vulnerabilities in a system, minimizing network exposure in order to make it harder to probe and exploit known vulnerabilities, and working with trusted sub-suppliers who work according to policies and processes that minimize flaws, and who provide patches and are transparent about discovered critical vulnerabilities.

Axis addresses the threat with the *Axis Security Development Model*, which aims to minimize exploitable vulnerabilities in Axis software; and with the *Axis Vulnerability Management Policy*, which identifies, remediates and announces vulnerabilities that customers need to be aware of in order to take appropriate actions. (As of April 2021, *Axis is a Common Vulnerability and Exposures Numbering Authority* for Axis products, allowing us to adapt our processes to MITRE Corporation's industry standard process.) Axis also provides *hardening guides* with recommendations on how to reduce exposure and add controls to reduce the risk of exploitation. Axis offers users *two different tracks of firmware* to keep the firmware of an Axis device up to date:

1. The active track provides firmware updates that support new features and functionalities, as well as bug fixes and security patches.
2. The long-term support (LTS) track provides firmware updates that support bug fixes and security patches while minimizing risks of incompatibility issues with third-party systems.

Supply chain attack

A supply chain attack is a cyberattack that seeks to damage an organization by targeting less secure elements in the supply chain. The attack is achieved by compromising software/firmware/products and luring an administrator to install it in the system. A product may be compromised during shipment to the system owner.

General questions

Recommended protections include having a policy to only install software from trusted and verified sources, verifying software integrity by comparing the software checksum (digest) with the vendor's checksum before installation, checking product deliveries for signs of tampering.

Axis counters this threat in a number of ways. Axis publishes software with a checksum in order for administrators to validate the integrity before installing it. When new firmware is to be loaded, Axis networked devices accept only firmware that is signed by Axis. *Secure boot* on Axis networked devices also ensure only Axis signed firmware runs the devices. And each device has a unique Axis device ID, which provides a way for the system to verify that the device is a genuine Axis product. Details about such cybersecurity features are found in the whitepaper *Cybersecurity features in Axis products* (pdf).

For more details about threats, see *Cybersecurity reference guide*.

What are vulnerabilities?

Vulnerabilities provide opportunities for adversaries to attack or gain access to a system. They can result from flaws, features or human errors. Malicious attackers may look to exploit any known vulnerabilities, often combining one or more. The majority of successful breeches are due to human errors, poorly configured systems, and poorly maintained systems – often due to lack of adequate policies, undefined responsibilities, and low organizational awareness.

What are the software vulnerabilities?

A device API (Application Programming Interface) and software services may have flaws or features that can be exploited in an attack. No vendor can ever guarantee that products have no flaws. If the flaws are known, the risks may be mitigated through security control measures. On the other hand, if an attacker discovers a new unknown flaw, the risk is increased as the victim has not had any time to protect the system.

What is the Common Vulnerability Scoring System (CVSS)?

The *Common Vulnerability Scoring System* (CVSS) is one way to classify the severity of a software vulnerability. It's a formula that looks at how easy it is to exploit and what the negative impact may be. The score is a value between 0-10, with 10 representing the greatest severity. You will often find CVSS number in published Common Vulnerability and Exposure (CVE) reports.

Axis uses CVSS as one of the measures to determine how critical an identified vulnerability in the software/product may be.

Cybersecurity Q&As

Questions specific to Axis

Questions specific to Axis

What training and guides are available to help me understand more about cybersecurity and what I can do to better protect the products and services from cyber incidents?

The *Resources* web page gives you access to hardening guides (e.g-
. *AXIS OS Hardening Guide*, *AXIS Camera Station System Hardening Guide* and *Axis Network Switches Hardening Guide*), policy documents and more. Axis also offers an *e-learning* course on cybersecurity.

Where can I go to find the latest firmware for my device?

Go to *Firmware* and search for your product.

How can I easily upgrade the firmware on my device?

To upgrade your device firmware, you can use Axis video management software like *AXIS Companion* or *AXIS Camera Station*, or tools like *AXIS Device Manager* and *AXIS Device Manager Extend*.

If there are disruptions to Axis services, how can I be informed?

Visit *status.axis.com*.

How can I be notified of a discovered vulnerability?

You can subscribe to the *Axis Security Notification Service*.

How does Axis manage vulnerabilities?

See the *Axis Vulnerability Management Policy*.

How does Axis minimize software vulnerabilities?

Read the article *Making cybersecurity integral to Axis software development*.

How does Axis support cybersecurity throughout a device lifecycle?

Read the article *Supporting cybersecurity throughout the device lifecycle*.

What are the cybersecurity features that are built into Axis products?

Read more:

- *Built-in cybersecurity features*
- *Cybersecurity features in Axis products* (pdf)
- *Supporting cybersecurity throughout the device lifecycle*

Is Axis ISO certified and what other regulations is Axis compliant with?

Visit the *Compliance* web page.

User manual
Cybersecurity Q&As

Ver. M2.3
Date: November 2023
Part no. T10189380