7 CYBERSECURITY BEST PRACTICES

2N
An Axis company

KEEP SOFTWARE UP TO DATE

Running devices with up-to-date firmware versions is inevitable when you want to mitigate possible cybersecurity risks.

When a manufacturer discovers a potential software bug, he fixes it in the next software release.

Installing software updates will ensure you utilize security patches for all newly discovered vulnerabilities.

2N
An Axis company

USE STRONG PASSWORDS

The least you can do as a user, is to create a c**omplex password that will not be easy to hack.**

Ideal password should consist at least of six characters. It should combine numbers, letters and symbols. Obviously, it´s not a good strategy to use easy-to-guess passwords as is a date of your birthday or a name of your hometown.

If you manage to create a strong password, fine. But **avoid sharing your credentials** with other users.

Even if you follow these rules, **it´s good to change your password** from time to time.

2N
An Axis company

DIFFERENT ACCOUNTS FOR DIFFERENT ROLES

It´s important to have multiple accounts with different privileges. A user will be limited to make only those changes that are related to his specific work tasks.

Again, even for these types of accounts, keep in mind to not share your password with anyone else.

This way you minimize the chance of spreading your secure credentials through out the company.

2N
An Axis company

LIMIT INTERNET EXPOSURE

To avoid malware, use **router-based firewalls** that reject suspicious traffic before it gets on the network. Of course, it is unthinkable to completely disconnect from the Internet. But it´s important to be careful and **protect the network with a strong password.**

Attackers are constantly scanning the Internet for machines that are exposed. If you want to know what is open to the network from the devices that you use, you can go to www.shodan.io and check it yourself.

The more devices you remove from direct Internet exposure, the more risk you reduce. Also remember to always **enable only the necessary product features.**

2N
An Axis company

SECURE THE NETWORK

a) **Create an independent network,** dedicated solely to those devices with sensitive information. Make it physically impossible to get into the network by having separate switches.

b) Use **virtual LAN (VLAN)**. VLAN contains isolated networks within the data center and each of the network is a separate broadcast domain.

c) Very useful is also securing the network thanks to I**EEE 802.1X protocol**. It prevents unauthorized devices from accessing the local network.

d) Make sure that manufacturers of devices or software that you use implement **protocols such are HTTPS, TLS, SIPS or SRTP,** enables by default. It also prevents so called “Man in the middle” type of cyber-attack.

2N
An Axis company

CHOOSE THE RIGHT PROVIDER OF REMOTE MANAGEMENT

It is very helpful to **manage all the installation sites from one single account.** No matter where the installation sites were, you´d be able to access them remotely from the comfort of your office. This might seem risky, having in mind all the dangers of exposing devices to the Internet described above.

Seek for a provider of remote management, whose service is based on secure cloud. In this case, **you no longer have to deal with router-based firewalls or tunneling**.

The cloud-based service will set an **encrypted communication itself.**

2N
An Axis company

SECURE THE IOT ECOSYSTEM

a) Create a **separate network for IoT devices**

b) choose a **strong router password** to protect the network

c) **never install any new electronics without checking its manufacturer**

d) don´t allow any unnecessary feature on the devices

e) and **update firmware and software** on a regular basis

2N
An Axis company