Five Tips For Hardening Your Security Devices And Networks

Several landmark ransomware attacks on enterprises in energy and food industries last year remind us that we are living in a world with constant cyber threats. Every industry has now been prompted to reinforce their network security and strengthen their online protections.
The security industry is no exception, as cybersecurity is also an on-going challenge for us, too. Here, we would like to offer some basic tips and practices to harden your network and keep your security devices protected.

1. CREATE STRONG PASSWORDS AND CHANGE THEM REGULARLY

You have heard it all before - almost every cybersecurity guidebook tells you that you need to create strong passwords. It is indeed a common instruction, but one of the most efficient methods to improve the protection of your network and devices. Passwords are just like lock on your front door, and if they are not strong enough, unwelcome visitors can easily crack them and "walk right in" to your network. Creating strong passwords is a very important first step in the process of hardening the security of your network and devices. For setting strong passwords, the following list provides some good principles to follow:

- Creating strong passwords is a very important first step in the process of hardening the security of your network and devices.
- CREATING STRONG PASSWORDS IS A VERY IMPORTANT FIRST STEP IN THE PROCESS OF HARDENING THE SECURITY OF YOUR NETWORK AND DEVICES.
- Include numbers, symbols, uppercase letters, and lowercase letters.
- Passwords should be more than eight characters long.
- Avoid any password based on repetition, dictionary words, letter or number sequences, usernames, relatives or pet names, or biographical information (birthdays, anniversary, etc.).
- Change your passwords on a regular schedule.

2. SET ONLY THE FIREWALL RULES YOU ACTUALLY NEED

A firewall intercepts all communications between you and the Internet, and decides if the information is allowed to pass through to your devices. Most firewalls, by default, will block all traffic both in and out. This is what we call "Deny all by default." In this default state, it is as if your devices are not even connected to the Internet. While this is a very safe state to be in, it is not very

useful. So, we must create a set of rules to tell the firewall what we consider safe. Everything else is, by default, considered not safe.
As you create rules to allow traffic in and out, you are creating tiny holes in your firewall for the traffic to flow through. The more rules you create in your firewall, the less secure your network becomes. You should only create minimum rules that you need, which can reduce risks of cyber threats through the firewall system.

3. UPDATE YOUR FIRMWARE IN A TIMELY MANNER

Firmware is the component that enables and controls the functionality of your network devices. It is a software program or set of instructions programmed right onto your network devices. It provides the necessary instructions for how your devices communicate with other computer hardware.

- Firmware updates are not just for bringing additional new features, but also often provide important security patches.
- FIRMWARE UPDATES ARE NOT JUST FOR BRINGING ADDITIONAL NEW FEATURES, BUT ALSO OFTEN PROVIDE IMPORTANT SECURITY PATCHES.

Firmware is the component that enables and controls the functionality of your network devices. It is a software program or set of instructions programmed right onto your network devices. It provides the necessary instructions for how your devices communicate with other computer hardware.

Firmware updates are not just for bringing additional new features, but also often provide important security patches. It is recommended that you always use the latest firmware so that you get the best possible security updates and most recent bug fixes.

4. ENCRYPT YOUR DATA

Another key way to safeguard your network and data includes using encryptions. This is the process of encoding your data in a way that can only be accessed through a corresponding decryption process. Data encryption is encouraged, as it keeps your data privacy safe from unauthorized hands - especially in the event of a data breach. Normally, it is not necessary to encrypt all of your data; you could make an encryption strategy to classify and assess risks of your data. Be sure to choose the right encryption tools for sensitive, non-public, and confidential data.

5. DEFINE CLEAR ACCESS PERMISSION POLICIES FOR ALL USERS

The right users need to have access to the right applications and data for organizations to function. It's necessary to make clear access permission polices for all users. You need first to define possible users who may access your network and security devices, and then set permission levels for each user to limit unnecessary access privileges and reduce the risk of cyber breaches.