DISTRIBUTED BY

madison
Technologies

Three Considerations for Managing the Security of your Industrial Network Infrastructure

MOXA®
Reliable Networks ▲ Sincere Service

Introduction

For almost every country, their economy and many other important services depend on a reliable critical infrastructure. As more and more countries are adopting trends such as the Industrial Internet of Things, their critical infrastructures are becoming more complex and are constantly connecting more devices and networks. While this expansion has numerous benefits and possibilities, this evolution is making their critical infrastructure more vulnerable to cyberattacks. As countries are becoming more reliant on their critical infrastructure, any cybersecurity breaches will put the countries' economy, public safety, and health at risk. Needless to say, the financial damage a cyberattack could cause is almost unlimited. In addition, any component supplier that has their components affected by a cyberattack is likely to suffer huge damage to their reputation, which will often result in them losing their current customers and make it difficult for them to find new customers in the future.

Overview of security on industrial networks

This paper will first provide some background regarding how to build a reliable network infrastructure before focusing on three important management guidelines that should be adopted if networks are to be kept secure throughout their network lifecycles. Below are the three guidelines that cybersecurity experts have identified that need to be considered in order to secure industrial networks.

- Manage who has access to the network
- Continually monitor and assess the security status
- Quickly respond to incidents and get networks back to normal when errors occur

Who is at risk of cyberattacks and why is it important?

There are numerous companies and governments that rely on their critical infrastructure. In order to highlight the importance of cybersecurity, examples from intelligent transportation systems and the oil & gas industry will be considered to demonstrate the damage that can be caused by not having good cybersecurity in place.

Intelligent transportation systems are vulnerable to a number of security threats that can cause serious disruption to the network, including unauthorized users gaining access to the network and changing configuration settings. These attacks can result in anything from cutting off power to trains so they are unable to move to closing down computer systems that monitor and control aviation traffic. Another example can be found in the oil & gas industry, where a person with malicious intent may obtain unauthorized access to the tank gauging system. Once an attacker has gained access to the network, they are in a position to manipulate the PLC to increase the tank filling limit, which could have disastrous consequences. For both of these industries, the networks involved contain hundreds or thousands of devices. One of the primary challenges for network operators is how to ensure that the configuration and security settings are accurate throughout the entire network lifecycle in order to reduce the risk of cyberattacks.

Two important considerations when building an industrial network

It is essential to have good security architecture in place to give operators the groundwork to be able to efficiently manage their network. A defense-in-depth approach is seen as the best option for securing industrial networks as it incorporates industrial secure routers, VPNs, and remote access solutions to help mitigate the risk of a cyberattack. After deploying a suitable infrastructure, the next step is to consider which devices to deploy. Hardened Ethernet devices have numerous advantages that include better security and higher reliability, which makes them suitable for deployment on networks where security is a high priority. For further details, the IEC 62443-4-2 standard includes guidelines for the technical security requirements of devices deployed on industrial networks. However, a network infrastructure that utilizes a defense-in-depth approach and deploys hardened devices that refers to the IEC 62443-4-2 standard is not sufficient to protect critical assets from cybersecurity threats. The ongoing monitoring and maintenance of the industrial network is essential to ensure that it remains secure throughout the entire network lifecycle. If you require more information, please visit our microsite.

The three easy to follow network management guidelines that help you deploy network device

In order to have a comprehensive set of industrial cybersecurity management guidelines, three factors need to be taken into consideration. The first is how to determine the identity of the person who is accessing the network and whether to grant them permission to access the network or change configuration settings. The second concerns how to constantly monitor and assess the security status of the network and devices. The third is how to ensure that any incidents are responded to almost immediately. These challenges, as well as the solutions and benefits, will now be considered in detail.

1. Verify the user and their authentication settings

The operator in charge of managing the network is responsible for ensuring the network remains secure after it has been set up. It is crucial to establish security management guidelines that include identity requirements, centralized authentication, and configuration management rules. The network operator must then follow these guidelines in order to enhance the security of the network.

Advice: Ensure Only Authorized Personnel Access the System by Using RADIUS and Sticky MAC Addresses

To secure against unauthorized users accessing and changing configuration settings, the Ethernet devices deployed on the industrial network should be compatible with Remote Authentication Dial In User Service (RADIUS). RADIUS is a protocol used on industrial networks to ensure that the user trying to gain access to the network has been granted permission to do so. RADIUS allows operators to maintain user profiles in a central database that can be shared across all remote servers. This provides a higher level of security because it allows operators to set up a network policy that can only be applied from a single administered network location. Performing network administration from a centralized location also makes it easier to track any activity that occurs on the network and to accumulate network statistics that can later be used for data analysis.

Sticky MAC addresses should be used in order to ensure that only authorized devices can access the network. When Sticky MAC addresses are used, only devices assigned to authorized MAC addresses have the ability to change configuration settings or send traffic through the network.

Benefits: Implementing RADIUS and Sticky MAC addresses allows operators to have a higher level of protection against users with malicious intent trying to gain unauthorized access to the industrial network.

2. Monitor and assess the security status

When the network is functioning, it is essential that network operators are constantly monitoring the network so that they are aware of the security status. However, network operators often find this tedious because little tends to happen for long periods of time. In order to combat this issue, any software or tools that can help network administrators gain visibility of the security status of their network will be beneficial to ensuring a secure network system.

Advice: Monitor and assess the security status by using MXview's Security View

MXview supports the Security View function, which helps operators easily monitor the security settings of Moxa's network devices on the industrial network. After starting MXview's Security View software, it will automatically scan the IEC 62443-4-2 related configurations of Moxa's network devices and determine whether the device is fulfilling the requirements of IEC 62443-4-2 level 2, level 1, or the basic level. The software is very easy to use and will quickly inform operators what the current security status is of each device on the network. The automatic scanning of devices' security settings ensures that all the devices, even on large-scale networks, have the appropriate security settings and removes the need for network operators to scan the devices manually, which can be a tedious and time-consuming task.

Benefits: MXview's Security View allows the security status of the industrial network to be checked automatically without requiring operators to have to perform the task manually or have any specialized IT knowledge.

3. Respond to incidents quickly

Ensuring network availability is one of the top priorities for network administrators. It is strongly recommended to record and store logs of every event that occurs on the network. If a cyberattack occurs on the network, the security incidents can be traced and the operators can respond to the event quickly and address the root cause of the problem as well as determine whether a threat still exists to the network. In addition, the configuration data for network devices should not be disclosed to third parties unless it is absolutely necessary in order for them to perform their job function. If the settings are changed by accident or on purpose and causes the network operator to lose control of the network, it could result in significant financial losses. Therefore, encryption of configuration settings and routine backup are essential to ensure the network can return to normal quickly if it falls victim to a cyberattack.

Advice: Rapidly respond to security incidents by utilizing a Job Scheduler tool that performs regular back up

Policies and procedures for controlling modifications to firmware and configuration settings are essential for every industrial network. The purpose of these procedures is to facilitate rapid responses to any security incident that occurs on the network and ensure that the information is protected against improper modifications prior to, during, and after the industrial network is up and running. However, it takes a lot of time and effort to routinely back up configuration settings, especially on large-scale networks.

The Job Scheduler tool included in MXview makes it easy to schedule a periodic backup of the configuration files by performing an automatic backup of the files on a daily or weekly basis at a time decided by the network operator. The automatic backup removes the need for the network operator to perform this task manually, which saves significant time and effort. In addition, MXview can also import the configuration files directly into devices located on the network, which means that recovery times are shortened if the network does experience downtime due to configuration errors.

Benefits: Getting the industrial network back to normal as soon as possible will reduce network downtime and also limit financial losses.

Conclusion

Before an effective management strategy for industrial networks can be implemented, it is essential to ensure that a defense-in-depth approach has been utilized and that hardened security devices have been deployed. After this has been achieved, the three key stages of the management network lifecycle should also be adhered to: verify the user and their authentication settings, constantly monitor and assess the security status of the network, and respond to incidents quickly.

Moxa provides a comprehensive solution that includes devices that are suitable to be deployed in a network architecture that utilizes the defense-in-depth strategy. Our devices refer to the guidelines set out in the IEC 62443-4-2 standard to help prevent unauthorized access as well as utilize RADIUS and Sticky MAC addresses in order to further enhance the security of the industrial network. In addition, Moxa's MXview network management software can be used by network operators to further enhance the security of the network as well as reduce the effort required from operators. For owners of critical infrastructure who take the threat of cybersecurity seriously, these solutions will help protect against cybersecurity threats and help reduce the costs that are likely to be incurred in the event that your critical infrastructure is infiltrated.

Learn more about our Network Management Software that help you secure your networks.