Seven Details Implementing Network Security Cheat Sheet

by [deleted] via cheatography.com/2754/cs/9561/

Introduction

Network security is absolutely necessary for today's industrial networks. Failure to restrict access can be disastrous. Access to your network by untrained persons can lead to misconfigured network devices. Access to unsecured ports can lead to network loops being accidentally created. Here are a few security details to keep in mind when constructing your network:

Credit: http://www.automationworld.com/seven-details-remember--when-implementing-network-security

1. Keep production running

Recovery and uptime are the critical priorities on the factory floor. Make sure security systems function in a familiar way so that people on the plant floor who are used to dealing with control systems can understand them. For example, don't create a security system that shuts down the equipment if a panicked operator enters the wrong password in an emergency situation.

2. Divide VLANs

Separate your production floor assets from the management functions (office computers, reception door locks, etc.) using different VLANs. It's often useful to divide the production network into three sections -- PLCs, HMI users and servers -- to reduce traffic where it is not required. Access to the management interface of your network switches can also be controlled. Utilize an accessible IP list to limit administrative access to your network devices. This list will only allow connections to the management interface of a switch from a list of pre-selected IP addresses. To further prevent access to the management interface, a separate management VLAN can be created for this purpose as well. However, many industrial networks operate in a single VLAN with a flat IP scheme. Creating separate VLANs can introduce a bit more complexity into the average system, but the accessible IP list can often provide just the right amount of protection along with the desired simplicity..

3. Use managed switches

Network Security

4. Guard against network loops

Many industrial networks are designed with redundant paths in the system and already employ a redundancy/loop prevention mechanism. This is also a feature of a managed switch. Without loop prevention protocols, any port can be connected with an Ethernet cable back into another port on a switch and create a broadcast storm. This can cripple the switch as well as the network. This kind of problem can also be tricky to track down and flush out of a network. Loop prevention protocols include the spanning tree variations such as rapid spanning tree. For industrial applications, these can be too slow, but optimized solutions such as TurboChain and broadcast storm prevention (BSP) can provide response time in milliseconds to prevent network loops from occurring. These features can be used to prevent a malicious denial of service outage from occurring as well as prevent an accidental Ethernet cable loopback..

5. Look for redundancy and robustness

Having equipment that is easy to disrupt makes an attacker's job easier. All network components, including cabling, cabinets and active equipment, need to be industrially hardened, resilient and have high mean-time-between-failure (MTBF) ratings because of the harsh environments found in an industrial facility. Active components in an industrial network, such as switches and routers, need to support industrial redundancy technologies and the level of redundancy required for your production needs. This will keep operations going in the event of malware or other network intrus-ions..

6. Early network warning system

Integrating security with industrial control systems is critical for both support and security event monitoring in a network. Using such a system will facilitate the detection of unusual activity on the network, an area that is typically poorly done in the industrial automation world. Plant personnel need to be immediately alerted if a read-only remote operator station suddenly tries to program a PLC. Waiting for the IT team to analyze the event the next day is too late.

7. Optimize Firewalls Protect the Right Protocols

Design your network with managed switches, which allow data flow control and reduce loads on the network. These devices contain a management interface that will give you great control over their operation, as well as limit access to the network.
Unmanaged switches do not provide any type of control and allow any device to be plugged into the network. Managed switches also allow the network designer to disable any unused ports. This prevents unauthorized devices from gaining access to the network. The ports can either be disabled or be configured to use a central RADIUS server, which can control access to them using 802.1X. This requires a bit more configuration, but allows for all your network devices to have a single user database that is centrally administrated, rather than have to manage usernames and passwords on individual switches. Make sure you change the default admin password of the switch. It typically comes set to a default and many fail to change it. It goes without saying that this is a big problem and it should always be changed..

Firewalls should be optimized to secure SCADA protocols such as Modbus and OPC, rather than email or web traffic, which have no place on a plant floor system. Products that inspect e-mail and web traffic simply add cost and complexity to the security solution. Design your security system to handle very wide power ranges, since the plant floor often has dirty power.