MAINSTREET IT SOLUTIONS

10 CYBERSECURITY TIPS FOR MANUFACTURERS

RISKS

NETWORK RELIABILITY

Reliability and security across firewalls, routers, servers, switches, and ICS equipment is essential.

INTELLECTUAL PROPERTY THEFT

Software platforms like PLM, ERP, and MES hold sensitive, proprietary data. As systems converge, your most precious assets take on higher cyber risks.

SECURE REMOTE CONNECTIVITY

The number of endpoints and individuals connecting to your network is growing. Vendors, employees, and other users need to gain secure, remote access to the network. Greater connectivity means greater risk.

1 SEGMENT THE ICS NETWORK AND CORPORATE NETWORK

There should be minimal access points between the two networks. By segmenting these networks, you substantially minimize vulnerabilities. Of course, there will be some instances where there will be connection points on the networks, but minimizing these connections makes it easier to look for suspicious behavior. Monitor traffic between the networks to find unusual behavior, such as an increase in sessions, session timing, and the types of connections.

2 INSTALL FIREWALL CONFIGURATIONS

Block unneeded and potentially dangerous traffic. Operational Technology (OT) protocols, such as Modbus, IEC 61850, ICCP, DNP315, etc., should never leave the ICS network segment. And while outbound email from the ICS network may be needed for alerting and notifications, there's no need for inbound email. Block inbound SMTP traffic to the ICS network. SSH, VPN, or other outside traffic; monitor, document and block unknown traffic. With both networks, segmented networks and specific traffic filters, allow better visibility to typical and atypical network traffic.

3 KNOW WHAT FTP CONNECTIONS ARE NEEDED AND USE SFTP

ICS networks are typically isolated and perform repetitive functions, therefore necessary FTP connections should be well known. FTP is a common data sieve. Avoid data FTP data loss by identifying and monitoring necessary FTP connections and use SFTP if possible.

4 LIMIT DNS REQUESTS OUTSIDE OF THE ICS NETWORK

The use of DNS in an ICS network is rare; reject DNS requests outside of the ICS network, and host files on local machines. Use host files on local machines.

5 DITCH DHCP AND USE STATIC IPS

DHCP simplifies and improves the accuracy of IP addressing, however it presents greater security concerns. Whenever possible, use static IPs. If a dynamic allocation is needed, monitor for rogue DHCP servers, ARP spoofing, and IP spoofing.

6 RESTRICT PHYSICAL ACCESS

Restrict physical access to the plant floor and the server room. Only essential personnel should have access to the plant or shopfloor, HMIs, or networking equipment. Consider biometrics to increase security and monitor systems access.

7 MONITOR REMOTE ACCESS

Vendors rely on remote access to access for diagnostics, repairs, systems improvements and more. Employees and partners need remote access to the shop floor and the network. It's important to know and track who has remote access permissions. Implementing two factor authentication ensures that only the right people are on the network. More importantly, monitor access and alert on unusual connections or activity.

8 MONITOR, LOG, AND AUDIT EVENTS ON THE NETWORK

Ensure network events are monitored, logged and audited. Identify FTP connections, IT and ICS connections. and remote access. Monitoring network events is a 24x7 activity. If you don't have internal resources available, consider outsourcing network monitoring to a managed security service provider.

9 SECURITY AWARENESS TRAINING

Your company can adopt the best security tools and processes, but employees will remain your greatest security risk. Introduce an annual security awareness training cadence to ensure employees understand policies for accessing the ICS network, acceptable use policies, security best practices, limitations, and permissions to manufacturing systems and the network.

10 PERFORM A RISK ASSESSMENT

Start with a risk assessment to identify, analyze, and evaluate risks within your network. Manufacturers have different types of risks than most organizations do. Industry 4.0 and IIoT trends make current manufacturing software, IP addresses and the IT and ICS network configurations a greater concern. Perform an assessment specific to these vulnerabilities then fill in the gaps with the appropriate technologies, processes, or solutions to minimize risk.

SCHEDULE YOUR RISK ASSESSMENT

(717) 354-8385 | SOLUTIONS@MAINSTREETITSOLUTIONS.COM