CYBERSECURITY

The Seven Strategies to Effectively Defend Industrial Control Systems

Henry Martel
Field Applications Engineer

antaira®
making connectivity simple...

Cybersecurity for Industrial Control Systems (ICS) has changed dramatically in recent years. The once considered trivial, inconvenient, and overlooked cybersecurity management features have transformed into a specialized security industry, specifically designed to protect industrial systems such as power plants, water treatment facilities, and transportation systems. Without cybersecurity using managed Ethernet switches for ICS, everyday conveniences such as having fresh drinking water or getting food from the grocery store would be impossible.

Historically, industrial networks have been simple standalone analog systems, with little to no outside communication beyond its meters, gauges, and control sensors. They were small, isolated, and closed looped with many in an “air gap” style configuration (physically disconnected from the enterprise network) with very little security.

Plant managers and engineers who operated these industrial networks viewed cybersecurity as a nuisance, and often avoided configuring user authentication and access permission settings. As such, the ICS were left unguarded with no security measures in place to protect them from outside attackers.

Today’s Industrial Control Networks

Industrial networks have grown in scale and complexity. Thanks in part to the Industrial Internet of Things (IIoT) revolution which introduced industrial smart I.P. based sensors, instruments, and networking devices. The once closed off standalone Operational Technology (OT) network developed into a robust, high-speed communication network requiring the same type of data link speed and backbone infrastructure as their Information Technology (IT) network counterpart. Therefore, the need to converge OT networks with IT networks became mandatory for IIoT IP based communications.

The convergence of these two networks meant greater flexibility and control over OT networks. This allowed administrators to create sophisticated OT networks by taking full advantage of IIoT smart devices for expanded communication, increased production, and optimized workflow.

Seeing the Unforeseen

The convergence between the IT and OT network has led to unforeseen detrimental repercussions. For instance, the lack of knowledge and experience needed for advanced security configurations to safeguard IIoT IP devices had a negative impact on the industry. The engineering mindset that once left analog OT networks open and unsecure is now responsible for securing advanced IP devices that reside on interconnected networks.

A neglected network runs the risk of increased security vulnerabilities allowing for a potential outside force to gain inside access. This situation can have severe consequences. The absence of cybersecurity has led to worldwide cyberattacks on critical infrastructures. There have been national and state-wide examples of launching cyberattacks against power plants, electrical grids, transportation systems, and major manufacturing operations impacting millions of people. Companies lost hundreds of millions of dollars in revenue from network downtime.

Recent ransomware attacks on two U.S. chemical companies Hexion and Momntive, along with Norsk Hydro -a global aluminum auto parts manufacturer, left hundreds of employees locked out of computer systems and critical processing systems. The cost of these cyberattacks was estimated to be over 80 million U.S. dollars.

In 2010, the now infamous Stunxnet cyberattack targeted the Iranianin Supervisory Control and Data Acquisition (SCADA) systems responsible for damaging Iran’s nuclear program. The computer worm was considered a cyberweapon built by American and Israel groups to impede the process of creating centrifuges for nuclear weapons. Since this event, adversaries have used similar types of cyberweapons against industrial control systems all over the world.

Global Solutions

Global leaders in the I.T. security sector, controller manufacturing, and government-sponsored organizations have formed various oversight groups to assist in the development of best practice methods and security specifications to help address this cyber threat.

In 2009, the U.S. Department of Homeland Security (DHS) created the Industrial Control Systems Cyber Emergency Readiness Team (ICS-CERT) to address cybersecurity for the industrial industries. In 2018, the Cybersecurity and Infrastructure Security Agency (CISA) was created with the mission to reduce cybersecurity threats and create a national hub for cyber and communications information, technical expertise, and operational integration. The CISA also established the Industrial Control Systems Joint Working Group (ICSJWG) to facilitate information sharing and reduce cyber risks on the nation's Industrial Control Systems (ICS).

Government agencies, oversight committees, and higher educational institutions are now recommending engineering students take computer systems and cybersecurity courses as part of their graduate studies. This approach ensures future generations of engineers managing and controlling ICS systems will have a basic understanding to the new threat landscape that awaits.

All of this resulted in the DHS and CISA creating a list of seven strategies to help protect, manage, and control industrial networks from cybersecurity. Below are the exact seven strategies DHS has written and put in place.

THE SEVEN STRATEGIES TO EFFECTIVELY DEFEND INDUSTRIAL CONTROL SYSTEMS

[U.S. Department of Homeland Security]

1. IMPLEMENT APPLICATION WHITELISTING

Application Whitelisting (AWL) can detect and prevent attempted execution of malware uploaded by adversaries. The static nature of some systems, such as database servers and Human-Machine Interface (HMI) computers are ideal candidates for running AWL. Operators are encouraged to work with their vendors to baseline and calibrate AWL deployments.

2. ENSURE PROPER CONFIGURATION / PATCH MANAGEMENT

Adversaries target unpatched systems. A configuration/patch management program centered on the safe importation and implementation of trusted patches will help keep control systems more secure.

Such a program will start with an accurate baseline and asset inventory to track what patches are needed. It will prioritize patching and configuration management of “PC-architecture” machines used in HMI, database server, and engineering workstation roles. Current adversaries have significant cyber capabilities against these management configurations, and infected laptops are a significant malware vector.

This program will limit the connection of external laptops to the control network and preferably supply vendors with known good company laptops. The program will also encourage initial installation of any updates onto a test system that includes malware detection features before the updates are installed on operational systems.

3. REDUCE YOUR ATTACK SURFACE AREA

Isolate ICS networks from any untrusted networks, especially the Internet. Lock down all unused ports. Turn off all unused services. Only allow real-time connectivity to external networks if there is a defined business requirement or control function. If one-way communication can accomplish a task, use optical separation (“data diode”). If bidirectional communication is necessary, then use a single open port over a restricted network path.

4. BUILD A DEFENDABLE ENVIRONMENT

Limit damage from network perimeter breaches. Segment networks into logical enclaves and restrict host-to-host communications paths. This can stop adversaries from expanding their access, while letting the normal system communications continue to operate. Containment provided by enclaving also makes incident cleanup significantly less costly.

If one-way data transfer from a secure zone to a less secure zone is required, consider using approved removable media instead of a network connection. If real-time data transfer is required, consider using optical separation technologies. This allows replication of data without putting the control system at risk.

5. MANAGE AUTHENTICATION

Adversaries are increasingly focusing on gaining control of legitimate credentials, especially those associated with highly privileged accounts. Compromising these credentials allows adversaries to masquerade as legitimate users, leaving less evidence than exploiting vulnerabilities or executing malware. Implement multi-factor authentication where possible. Reduce privileges to only those needed for a user's duties. If passwords are necessary, implement secure password policies stressing length over complexity. For all accounts, including system and non-interactive accounts, ensure credentials are unique, and change all passwords at least every 90 days.

Require separate credentials for corporate and control network zones and store these in separate trust stores. Never share Active Directory, RSA ACE servers, or other trust stores between corporate and control networks.

6. IMPLEMENT SECURE REMOTE ACCESS

Some adversaries are effective at gaining remote access into control systems, finding obscure access vectors, even "hidden back doors" intentionally created by system operators. Remove such accesses wherever possible, especially modems as these are fundamentally insecure.

Limit any accesses that remain. Where possible, implement "monitoring only" access enforced by data diodes, and do not rely on "read only" access enforced by software configurations or permissions. Do not allow remote persistent vendor connections into the control network. Require any remote access be operator controlled, time limited, and procedurally similar to "lock out, tag out." Use the same remote access paths for vendor and employee connections; don't allow double standards. Use two-factor authentication if possible, avoiding schemes where both tokens are similar types and can be easily stolen (i.e; password and soft certificate).

7. MONITOR AND RESPOND

Defending a network against modern threats requires actively monitoring for adversarial penetration and quickly executing a prepared response. Consider monitoring programs in the following five key places:

1) Watch IP traffic on ICS boundaries for abnormal or suspicious communications.

2) Monitor IP traffic within the control network for malicious connections or content.
3) Use host-based products to detect malicious software and attack attempts.
4) Use a login analysis (i.e; time and place) to detect stolen credential usage or improper access, and verify all anomalies with quick phone calls.
5) Watch account/user administration actions to detect access control manipulation.

Have a response plan for when adversarial activity is detected. Such a plan may include disconnecting all Internet connections, running a properly scoped search for malware, disabling affected user accounts, isolating suspect systems, and an immediate 100 percent password reset. Such a plan may also define escalation triggers and actions, including incident response, investigations, and public affairs activities.

Have a restoration plan, including having “gold disks” ready to restore systems to known good states.

Summary

Industrial industries and the people, communities, and entities they serve are facing greater risks from cyberattacks.

Administrators and engineers who service industrial networks must be diligent in providing security measures to safeguard against attacks. As copious amounts of advanced communications find their way into OT networks, vigilant attackers will be ready to penetrate with more advanced tools, techniques, and procedures.

Security threats to industrial networks are a global issue. Government officials, industry leaders in I.T. security, and representatives from industrial industries have created a working set of standards and guidelines for securing industrial control systems.

Works Cited

Seven Steps to Effectively Defend Industrial Control Systems [U.S. Department of Homeland Security] (n.d.) Retrieved September 15, 2019, from Department of Homeland Security NCCIC