Education is Essential for ICS Cyber Security Preparedness

Author: Daniel Ehrenreich, Consultant and Lecturer, SCCE

Introduction

Cyber security awareness for Industrial Control Systems (ICS), also known as Operating Technology (OT) , is highly important for managing water and electricity supply, transportation, communications and manufacturing facilities. Effectively educating the control engineers and users on ICS-OT cyber security risk can be done through well-defined preparedness. The education program shall involve a) ICS operators and experts, b) IT experts who want to learn ICS basics and cyber defense solutions and c) managers who must make correct decisions related to allocation of resources. This paper highlights few important processes and allow you effectively achieving these goals.

Differentiation among IT and ICS zones

IT cyber security experts who are understanding the ICS cyber security, shall learn the basic principles related to control processes to effectively deal with ICS Cyber security.

- Prior dealing with cyber physical operations, they must study the ICS architecture as described in layers 0-2 of the Purdue Model. While the goal of IT experts is focusing on assurance of Confidentiality-Integrity and Availability (CIA), the true goals of ICS experts are focusing on Safety-Reliability and Productivity (SRP). Therefore, ICS and IT zones must be built and commissioned separately and NOT converge.
- While the role of IT experts includes frequent patching and updating of their systems, ICS experts cannot do that, as every change represents a risk to the SRP. While there is no single cyber defense method which may absolutely prevent an attack on the ICS, the best you can do is deploying layered cyber defense combining all vectors of the PPT Triad (People, Processes, Technology.
- Cyber defense measures for IT and ICS-OT architectures must be different. For example, a penetration test to an IT system, it worst case might cause a temporary shutdown, conducting penetration testing on an ICS might interfere with the controlled process and lead to outage, damage and even risk to lives.

Analyzing the risk factors

Understanding the cyber-attack surface and the vectors is among the key principles and allows predicting most paths which an attacker may consider. For achieving more granular and as accurate as possible prediction, you may use the Industrial (Lockheed Martin) Cyber Kill Chain as well as the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) principles introduced for ICS in 2020.

- ***Non-attack risk factors:*** First you must consider two incidents which might risk the ICS process, cause unexpected operation outage or damage but are not considered as a real cyber-attack; a) failure of an ICS sensor, a PLC, a communication appliance or an unexpected software bug, and b) incorrect action done by an authorized person. All these might lead to a panic response by the ICS-OT operator.
- ***Negligent behavior of people:*** You must consider actions such and inserting a not-certified USB stick to the ICS network, failure to detect a social engineering action, negligent supply chain processes, allowing remote connection to the ICS without authenticating the connecting person and his computer, consistent use of simple or repeating passwords, poor physical security, and more.
- ***Intentional attack by an insider:*** Such adversary might use his knowledge and attack the ICS directly or through the IT network, manipulate the Enterprise Resource Management (ERP) process, alternate parameters on utility processes; HVAC, data center cooling, UPS, fire alarm, in buildings, etc.
- ***Attacking the ICS Network:*** Direct access to the ICS network through a “Backdoor” connection, conducting Man in the Middle (MitM) access, using a spoofed identity, DDoS attack, compromising the firewall between the IT and ICS networks, leaking out information from the ICS, etc.

- ***Manipulating the ICS process****:* Considering direct sabotage on the HMI, Engineering station, PLCs, field sensors, synchronizing GPS or NTP, manipulating the process through APT attack, exploiting Zero-Day vulnerabilities, etc. These actions are capable causing outage and damaging the machinery.

Methods for ICS cyber defense

Deployment of an effective cyber defense on ICS-OT shall be based on the overall risk factor, calculated by the likelihood of an attack and the harming impact (R=I*P). Consequently, the PPT Triad-based defense method shall be defined according to the architecture, data protocols, utilized communication media, etc.

- Allow performing antivirus and other updates on the ICS only after intensive safety testing.
- Conduct periodic cyber security assessment for detecting new vulnerabilities for the entire ICS.
- Strengthen the perimeter security particularly for all installations which attackers might access.
- Deploy strong segregation among the IT and ICS zones and among unrelated control appliances.
- Prioritize use of ICS oriented FWs, DMZ, Data Diode, SIEM, white-listing programs, etc.
- Use IDS for detecting ICS-related anomaly conditions at Purdue Model levels 0, 1 and level 2.
- Deploy strong authentication (such as 802.1X) prior connecting any device to the ICS network.
- Perform in-depth inspection of all files and media prior transferring them to the ICS network.
- Always supervise the remote access process and block the connection a.s.a.p. after completion.
- Adhere to the ISA-IEC 62443 international standard and regulations for ICS Cyber security

Educating your staff on cyber security risks

Cyber security experts know well, that high % of “successful” attacks were possible due to lack of awareness and experience in their organization. Therefore, periodic and well-tuned education for all personnel shall be a mandatory action for achieving ICS Cyber security posture. Among employees who shall participate are; a) System operators and ICS maintenance engineers who must upgrade their cyber security skills, b) IT cyber security personnel who must learn how ICS operates and how it can be protected and managers and decision makers who must understand this topic for properly allocating resources.

The training program must include sessions on the ICS applications and architecture, description of risks to the ICS components and periodic drills with demo illustrating an attack-process. The corporate CISO and the management shall clearly define responsibilities for dealing with the following post-incident tasks:

- Instant attack mitigation, blocking the lateral expansion of the attack and minimizing damages.
- Collection of detailed forensics-related data on the attack details and reporting to all stakeholders.
- Effective and rapid activation of DRP for restoring the operation according to the defined BCP.

Summary

Industrial organizations must have documented and practiced methodology for dealing with cyber incidents. ICS cyber security experts must have the knowledge and experience for supporting their organization. These actions will help you complying with industry regulations and preventing incidents that might risk lives of people, cause operating outages and damage to machinery. Therefore, the managements shall allocate adequate resources and acquire the need expertise for effectively dealing with cyber security.

@@@@

Daniel Ehrenreich, BSc. is a consultant and lecturer acting at Secure Communications and Control Experts, and periodically teaches in colleges and present at industry conferences on integration of cyber defense with industrial control systems; Daniel has over 29 years’ engineering experience with ICS for: electricity, water, gas and power plants as part of his activities at Tadiran, Motorola, Siemens and Waterfall Security. Selected as the Chairman for the ICS Cybersec 2021 conference taking place on 11-2-2021 in Israel. *LinkedIn*