SECURICON
Information Security Solutions

Industrial Cybersecurity in 2020: How to Conduct An OT/ICS Gap Analysis

Introduction

In a recent blog post, The 5 Big Risks for Industrial Control Systems in 2020, we talked about some of the risks that Industrial Control System (ICS) owner-operators will face this year: from IIoT attack vectors to increasingly sophisticated hackers with knowledge of Operational Technology (OT) protocols and vulnerabilities, there's never been a greater need for industrial cybersecurity than there is today.

As it turns out, the industry is very aware of this fact, but not everybody is prepared to do something about it. Various industry reports from 2018 to today indicate that an overwhelming majority of organizations are concerned about OT/ICS security – yet, under a quarter of their employers were compliant with industry and government regulations regarding industrial cybersecurity at that time.

The Dangers of Complacency

This complacency is a disturbing problem not only for organizations, but also for the nation: without serious attention to OT/ICS security, countries are at heightened risk for critical infrastructure attacks like the one which left millions of Ukrainians without electricity in 2015.

In 2020, we hope to see organizations taking industrial cybersecurity more seriously than they have in the past. Fortunately – with a solid understanding of the risks they're facing, and a simple gap analysis – fortifying OT/ICS systems against their most dangerous adversaries is not difficult.

Gap Analysis for OT/ICS

Most security professionals will understand gap analysis from the context of IT and standard cybersecurity. As the basic starting point for any security strategy, a gap analysis reveals high-level areas where an organization's security position can be improved through investment and future development.

Here are the basic steps:

- DETERMINE IDEAL SECURITY POSITION – **the "desired state" -- identify controls, systems, training standards and other measures relevant to an ideal security position.**
- GAUGE CURRENT SECURITY POSITION – **the "current state" -- assess the current security position of your organization, highlighting areas where it falls beneath the standard.**
- SET ACTIONABLE GOALS – **determine and schedule actionable changes that can bridge the gap between your present security position and the ideal; and develop a detailed plan to implement these changes over a defined period of time. And keep in mind that it's a moving target!**

Few organizations will perfectly meet the ideal standards for security in any given domain, a gap analysis will keep their spending and strategy focused on the right path, which is mitigation of vulnerabilities to stay ahead of evolving risks.

Basic OT/ICS Security Standards

Since the first step of a gap analysis is to identify the ideal security position, let's cover the basics of industrial cybersecurity from the standpoint of proactive risk prevention:

- **Up-to-date and well-supported technology, operating systems and protocols**
- **Strong security controls with network segmentation and air gaps where possible**
- **An incident-response strategy with thorough remediation procedures for any major threat incident**
- **A competent team of ICS-literate professionals with the ability to identify vulnerabilities and respond rapidly to carry out an incident-response strategy**
- **An accurate asset inventory and asset management tool for rapid retrieval of information**

Gaps in an OT/ICS security position emerge whenever one of these points is neglected, and it would be impossible to develop an arbitrarily long list of examples. Instead, we'll focus on the most common ways that we see organizations falling short of the goal.

ICS-Specific Gaps

1. INACCURATE INVENTORY

According to one survey, 61% of ICS owner-operators are not confident in their ability to find information about assets quickly. This is a problem with inventory management: an incomplete or out-of-date inventory – and inventories spread across disjointed systems – will be difficult to locate for vulnerability analysis, servicing and remediation of threats.

2. POOR VENDOR IMPLEMENTATIONS

Products that do not provide adequate functionality, fail to integrate with other systems or require constant maintenance may indicate poor configuration by the vendor, or the need for servicing/replacement. Depending on the asset, the security risk presented can be severe.

3. LACK OF SECURITY CONTROLS

Security controls take many different forms, and common oversights include:

- **Assets that have not been updated from default vendor settings**
- **Lack of network segmentation**
- **Insecure protocols: legacy and open-source protocols are particularly vulnerable since they are well known to attackers, and – in most cases – might not receive updates or patches to fix security issues**

Remember that a lack of security controls in one domain may suggest a lack in the other: administrators should consult resources like the NIST CSF when identifying and developing controls to implement.

Culture Gaps

1. CHANGE-AVERSE ORGANIZATIONS

Because the modernization of OT is a relatively new phenomenon, change-averseness disproportionately affects OT-dependent organization: 53% of ICS networks across the world are running on a version of Windows (7, XP, 98, etc.) that is no longer supported by Microsoft.

2. LACK OF ICS LITERACY

ICS professionals are scarce, so it's no surprise that many organizations lack confidence in their employees to support, service, maintain and adequately assess OT/ICS systems.

3. BAD VENDORS

Naturally, the relationship between product vendors and OT is potentially more important than it is in some domains. Bad vendors can therefore worsen an organization's security position in multiple ways:

- **They are slow to provide updates/patches, or outright refuse to**
- **They require approval for or disallow the use of 3rd party software on their products**
- **They do not honor service agreements**

Resolving ICS/OT Gaps

After identifying gaps in your industrial cybersecurity position, remediation can take many forms: lack of ICS-literacy can be improved with training, bad vendors can be eliminated in favor of alternatives, and a lack of adequate security controls may require a comprehensive risk analysis to better understand the problem.

There is no one-size-fits-all answer to OT security, but taking the time to learn about the risks facing your organization is a first step towards making your operational technology safer in 2020. Two years ago, Kaspersky said that over 40% of ICS systems for which they had data were attacked: now is the time to make sure that next year's statistics won't include you.

SECURICON
Information Security Solutions

Toll Free: 877-914-2780
www.securicon.com
info@securicon.com

5400 Shawnee Road
Suite 206
Alexandria, Virginia 22312