IndustryWeek

TOP TIPS

Six Steps to Take When Implementing Industrial IoT Security

The gaping holes in corporate security are well documented and many companies are addressing them. However, most discussions about implementing industrial Internet of Things (IoT) security merge it with enterprise security, which makes the process even more difficult than it needs to be. To help, the following six points describe the very first steps you should take to ensure security when starting any industrial IoT implementation.

1. Establish a team dedicated to security.

The team should encompass representatives from global information security, IT, engineering, operations, and the vendor or vendors chosen to be the primary external supplier of resources and security expertise. Remember, these vendors will likely remain an essential part of your IoT team for a long time, so they should be considered no differently than your internal staff. That being said, be sure to conduct a security audit to determine if these companies or consultants meet your requirements now and have the resources to grow along with your company.

2. Produce an inventory of your industrial assets.

It's impossible to move forward with developing industrial IoT security without first knowing what assets may or may not be affected. The effort required obviously depends on how extensive these assets are, and if you have multiple facilities to consider, tackle each group and location individually. The information you collect should include detail about all machines, the number of machines that have the ability to communicate local or beyond (and using what protocols), and others specific to each group or facility. This activity is vital to industrial IoT security success because it provides the information required to perform all other activities in industrial IoT deployment. So, it should be very comprehensive, regardless of how much time it requires.

3. Decide what equipment really needs to be connected.

A good rule to follow is that any machines or other equipment which do not serve the company's interests by being connected to the Internet, shouldn't be. The results of an analysis based on this assumption will show that some will not serve the company's interests—even some that may already have Internet access. Intelligence is moving toward the edge of the network. One of the benefits of edge computing is the potential to increase network performance by reducing latency.

4. Identify the missing links and tap into people that have more extensive experience with security than you do.

Some of the ways that hackers can gain access to a device, machine, or computer are readily apparent, but others are not obvious. So, you always should complement your IT staff with consultants whose expertise is directly related to cybersecurity and who have years of experience as well as knowledge of current threats and scenarios, as things change frequently. Collectively, this team can identify all "ports of entry" and determine how to best seal them.

5. Learn about connecting legacy equipment.

Industrial equipment is built to withstand the rigors of the production environment for many years or even decades. So, it's likely that some of the equipment on your list has minimal connectivity capability or possibly none at all. Fortunately, as more companies implement industrial IoT, solutions are available from various sources to help solve this problem. Typically, hardware is made "connectable" by adding wireless-enabled sensors and software, and these solutions almost invariably address security. The best approach depends on many factors, such as the age of the machine and the software that runs it, and if it already has some ability to communicate. It's likely, though, that this equipment will need particular scrutiny as it's being brought online, as it will not have the latest security features.

6. Determine if some machines, computers, or other equipment should be replaced.

Although retrofitting existing (and typically expensive) hardware is comparatively simple and can be comparatively inexpensive, there are other factors to be considered as well. For example, if the financial resources are available, it often makes sense to replace legacy equipment, for several reasons. A new machine will invariably have at least one type of modern onboard connectivity as well the latest security features and will run on standardized software.

Summary

It's not surprising that large-scale industrial IoT deployments are an increasingly appealing target for cybercrime. They have hundreds, even thousands, of possible points of entry (the attack surface), from wireless-enabled sensors at the edge through the industrial IoT gateway and outward to the cloud. Only by scrupulous attention to every one of these points can security be reasonably assured, and this requires more than the minimal password maintenance, firewalls, and other fundamental tools.

The process is hampered by many factors, most notably by the fact that IoT itself is new and there is no single standard or overarching set of standards that define it. In addition, many of the industrial IoT's constituent parts were not designed to be inherently secure and sometimes don't have the memory or other resources to implement security, there are numerous (often incompatible) wired and protocols in use, and a long list of other concerns. That said, of all the elements in an industrial IoT deployment, security will prove to be the most important in the long term, and the time and money required to implement and maintain it will be well spent.

This content was developed together with Siemens Digital Industries Software.