Cyber Security in OT

Asim Farooq

National Technical Sales Consultant

Schneider Electric

10900 Equity Drive

Houston, TX

Introduction

Advancement in technology has no doubt given us an edge in making our lives better and more productive. We can preempt health related concerns by providing diagnoses before they become an issue. We can extract natural resources with more efficiency and with less impact to the environment. We are even able to access conferences and lecture materials remotely in the comfort of our homes. With the push to get these advancements into our daily lives and even into an industrial plant, "security" though essential, is sometimes a beast of a task to maintain! Many have not thoroughly considered the effects of bringing industrial data to our fingertips and then having to keep it updated. Why update it? Well, the data is not only accessible for the "right" user, but it is also accessible to the "wrong" user without keeping pace with the changes in technology.

Analog to Digital

There was a time when the world used to function on rotary phones, face to face meetings, writing letters with a pen and paper, and chart recorders. One had to be present at the specific location to get tasks done. Though some of these analog methods still exist, they are being upgraded or replaced with digital formats in the quest for personal ease. Advancements have been made to introduce even more devices with unique identities connected to the web or also known as Internet of Things (IoT). These devices include smart phones that allow you to read/write email and browse the web, computerized cars that can help drivers stay in their lanes and warn of possible threats ahead of time, refrigerators that can tell you if you are low on milk, and when it comes to talking to people, we use whatsapp, facetime or snap chat or text each other, even in the same house.

IoT transitions in to IIoT

From the industrial side, vendor implementations involved proprietary devices and communications that were locally connected with little or no remote access. Any code or firmware changes required a physical person to attach to the device and update it, costing time and money. It was just a matter of time before the benefits of IoT were recognized and transitioned in for industrial use. Hence the Industrial Internet of Things (IIoT) was introduced, where all the PLCs/RTUs, Sensors, communications were interfaced via networks, allowing not

only for a reduction in the time it took to get data back from the various sites, but also allowed for any user to connect and see the data in real-time from anywhere in the world. The real-time data has allowed many businesses to stay head of the demand and be pre-emptive in production and transportation of resources and materials.

Security concerns

As “cool” and “convenient” as it may be to have data available at the fingertips, there is the other aspect of having access to all the data on the web that everyone is oblivious of. Security.

Let’s start from the analog days: what are ways to eavesdrop on conversations? Being an ear shot of the conversation or using a glass against the wall from the other side of the room. How about trying to read the handwritten letter? One physically had to intercept the letter between the time it was written to the time it was read by the receiving person. Not so easy. Now that we are in the digital era, is the digital communication more secure? Let’s see: what is the only way to breach a conversation on your cell phone? Not just one way to breach it and not just from one spot! You could be anywhere in the world and hear in on a conversation with the right digital tools under your control! How would you breach an email? Just like the conversation, you could do it from anywhere in the world.

Now that we have determined that breaches in a digital world is much easier, let us look at the impact of what the breaches can do. What is the worst-case scenario for someone whose identity gets stolen? There would be possible financial losses and the credit worthiness would take a beating, especially when trying to lock in that low interest rate. In summary, the individual’s life would get miserable for some time till they get it all sorted out. Now take the security concern from an individual to a company. What is the possible negative effect? It is not just one! There could be financial loses, credibility of the company, layoffs causing economic hardships to individuals and the community, and potential loss of life. Let’s tie this to a hypothetical example; an electric utility company has a security lapse and hackers take advantage of it by infecting all the equipment with a virus and hence bringing down the whole grid. Not only did the company lose credibility, financial loses, but potentially may have put millions of people in danger because of the loss of power. What would happen if the hospitals lost power with patients in the ICU? How would you fill up your car with gas or charge the EV? Who would you call to complain about the power outage, since the cell network is probably also down due to the power outage? The minor inconvenience to an individual’s reputation may seem small compared to what a company has to deal with. In reality, they both are a serious cyber security issue.

The figure below shows the gradual increase of malware attacks over the last 10 years.

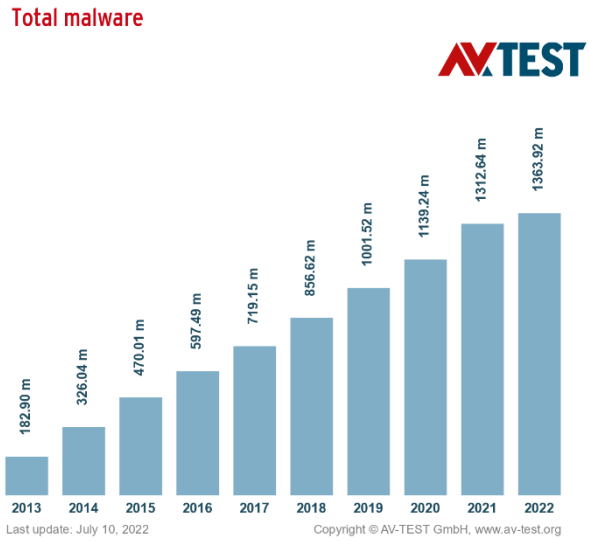

Figure 1: Malware attacks

Now let's look at the number of new malwares being created for that last two years.

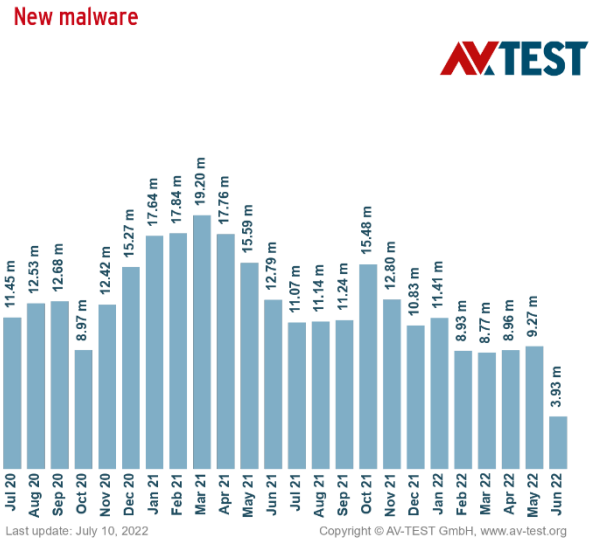

Figure 2: New Malware software

You can see a decrease in the number of new malwares. This is partly due to the fact that current technology only allows so many variations before it reaches it limits. At least until a new tech comes on the scene. This is not meant to scare the "right" people to regress back to the days of analog communication, instead it is to better understand what does moving to an IIoT environment means and how to better protect yourself from the "wrong" people.

Recommendations

Now that we better understand what advantages and disadvantage IoT and IIoT bring to the table, we can work towards a solution that will allow us to keep moving forward with the correct precautions in place.

The first step is to get Information Technology (IT) staff to better understand the workings of Operational Technology (OT) environment. IT members work on the business priority of confidentiality first by locking down everything, which does not work the same way for the OT side of Supervisory Control And Data Acquisition (SCADA). SCADA's priority is to be able to get to the data all the time because all aspects of the operations require the data to operate efficiently. The data does have certain ports that it needs to go through, and IT can lock down everything but those ports without effecting the SCADA system. Better yet, find vendors that allow you to change the ports for the standard protocols. For example, everyone knows that Modbus TCP uses port 502 (yes even the right hackers). If the vendor of the hardware allows you to, change the Modbus TCP port from 502 to something else (yes, some do. Just make sure you document the changes for audit reasons.)! It is just another thorn that hackers must figure out to get around the security implemented. The more thorns in the way, the more likely they will move on to the next system.

IT also needs to understand that regular unscheduled updates to the network devices and operating system cannot be done to the OT environment, as it affects how the devices communicate with each other. Setting guidelines and procedures for how IT should handle OT assets will help in the long run.

Once an IT / OT collaboration has been developed, we can then move on to what recommendations/standards to follow for safe guarding the SCADA. Based on your type of business, you could fall in to one or multiple of the following standards:

- NERC – North American Electric Reliability Corporation
- API - American Petroleum Institute
- ISA – International Society of Automation
- AWWA – American Water Works Association
- Etc

If your company is not sure what standard(s) or regulation(s) to implement, ask the device vendor for assistance. Many of the vendors have Cyber teams that can help you not only assess but design and maintain OT cyber security in conjunction with IT's help.

Typically, the implementation of the security will involve breaking the various aspects of the SCADA and Enterprise network into zones that are separated from each other with network hardware that function as security firewalls. Based on the zone, they can be designed to communicate one way or bi-directional with other zones. You would also design the zones in such a way that a device from one zone may not traverse through multiple zones. The

temptation of wanting to zone every piece of the equipment and area in its own cyber bubble, does need to be avoided. The point is to secure the area, not make it impossible for data to move from one area to another.

The two figures below show a typical system without any security (left) and one with properly segregated security zones using firewalls (right).

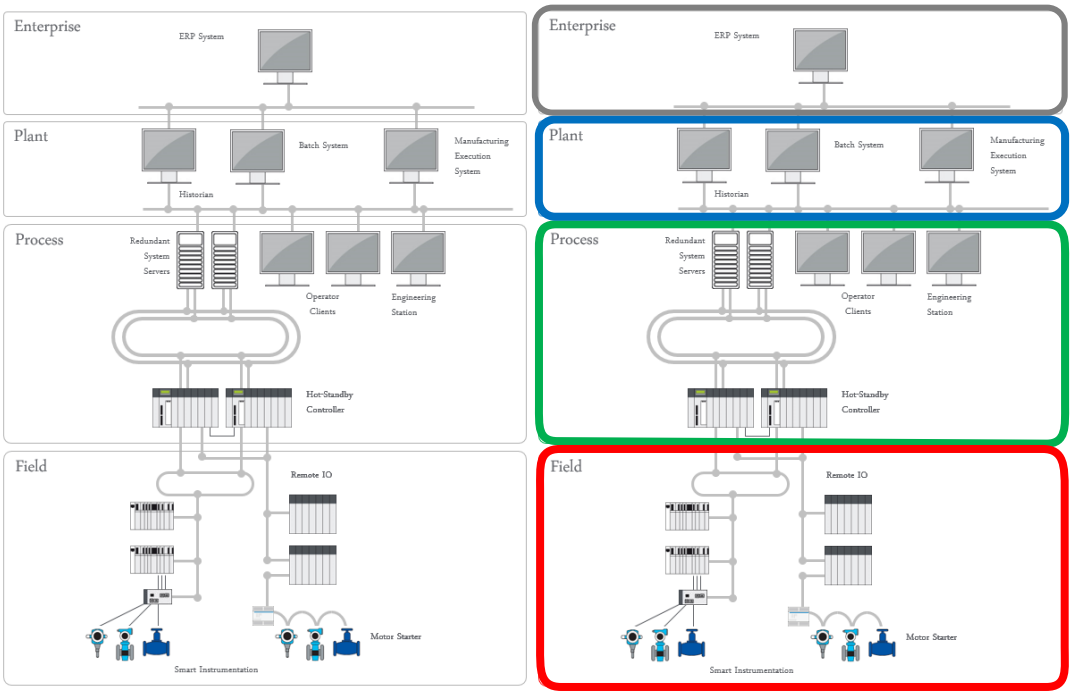

Figure 2: Open SCADA network (left) vs Zoned off SCADA network (right)

Continued updates and education

You finally got IT and OT working together and a secure implementation is in place. Or is it? Nope. Now a plan is needed for when and how to update the network/SCADA firmware and to implement any Vendor approved operating system patches. These updates are needed so that any open exploits are not taken advantage of by hackers.

Having a plan for patching in place now allows for the training and continued education of the employees. Here is a short list of topics that can be discussed:

- not to share their passwords with others
- not to take selfies and post on their social media accounts
- how to recognize a phishing email and to report it to the right IT team
- not to install USB devices from one zone into another
- not to use the USB port on devices to charge their phone!
- Etc

Ralph Waldo Emerson said: “Life is a journey, not a destination”. In similar fashion, Cyber Security is a journey, not a destination.

Conclusion

The discussion in the paper is meant to simplify the reality of the digitization in the industrial applications and what to plan for from the security side. There is no right solution for all situations but a combination of various recommendations and implementations from prior lessons learned. Quick and easy access is needed to the data but not only is that data easily accessible by the “right” user, it also is accessible to the “wrong” user. There is a living balance to becoming effective and productive while being secure. The question is finding where is that balance! Happy securing!