SCADA and Cyber Security: The Year of Action

By Eric Teichmiller
Eric.Teichmiller@h2lsolutions.com

SCADA and Cyber Security: The Year of Action

EXECUTIVE SUMMARY

With Defense Federal Acquisition Regulation Supplement (DFARS) fresh on everyone's mind, it is important to remember that there are still other areas that Cybersecurity can improve. Standards for Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) have been in place for some time, but have not been strictly regulated. The National Institute for Standards and Technology (NIST) released 800-82 originally in 2011, which was superseded by Revision 1 in 2013 and was then superseded by Revision 2 in 2015.[1] To compliment these standards, industry organizations are creating supplemental standards of their own such as the North American Electric Reliability Corporation Critical Infrastructure Protection for Electric, Chemical Industry Data Exchange/American Chemistry Council for Chemicals, among others.

The Department of Energy released a nearly 500-page report in early 2017 warning of an "imminent" threat to the electrical grid. With a number of cyberattacks over the last several years, this comes as no surprise. The ICS cyberattacks in 2016 that threatened the Kemuri Water Company, proved that a threat against ICS could be disastrous. If the attackers chose to push their limits, or had had more capabilities, the outcome may have been lethal. Because of the multiple warnings and threats of cyberattacks, 2016 became the year of "if" according to the ICS Cyber Security Conference.[2]

In 2017, so many systems moved away from analog and adopted TCP/IP solutions which left ICS systems vulnerable to the same exploits as other cyber systems utilizing these features. It was this transition that lead to 2017 being labeled the year of "truth."

When utilizing sensors, the authenticity of the data received is paramount. The danger that we faced in 2016, in the year of "if", is known as data forgery. If the data we received that alerted us to this incident was not truthful, the attack would have gone unnoticed. With this, 2018 should move forward as the year of "action".

With cybersecurity being closely analyzed and improved upon in government and financial industries, SCADA and ICS will need to undergo the same treatment. As cyber continues to evolve and become more integral in our everyday lives, the hardening of systems across all industries will need to be brought up to new standards as specified in the NIST 800-82. Companies should review and adhere to the NIST 800-82 set of regulations and standards and integrate these standards vertical to your organization.

To assist with adhering to standards, the Department of Energy has released a simplified 21 Step Guide to becoming more secure which will be covered in the next section.[3]

STEPS FORWARD

The Department of Energy's 21 Steps shown below take just a handful of things into account – most important among these is awareness. Several of the steps simply require you to know what and who you have on your network, and hardening those aspects. Your organization should also be aware of what devices are on your network, know what devices connect to the systems remotely, and verify that the connections are handled in a secure way.

Others include ensuring that:

- all unneeded ports or services are disabled and the ones in use are up-to-date.
- any built-in security features have been configured and are not set to factory defaults.
- any factory built-in backdoors are known and that all passwords are up-to-date.
- all personnel are aware of their role, practices are in place, and that adherence to all those practices are followed.

Another critical component is to implement a strong network architecture with the concept of defense-in-depth in mind. As a best practice, you need to keep as much of the network segregated based on role as possible and monitor the network segments for abnormal traffic separately to ensure that any incidents remain isolated.

Awareness and diligence can ensure that all aspects of the network stay up to standards and are kept patched for new security risks. Your organization will need to perform routine scans of the network to identify any issues. Additionally, it is recommended that you perform penetration testing both within the network and from the outside. A penetration test should be conducted on the site itself to demonstrate that all physical security is performing to standards.

Below are the 21 Steps as outlined by the Department of Energy for your review:

1. **Identify all connections to SCADA networks.**
2. **Disconnect unnecessary connections to the SCADA network.**
3. **Evaluate and strengthen the security of any remaining connections to the SCADA network.**
4. **Harden SCADA networks by removing or disabling unnecessary services.**
5. **Do not rely on proprietary protocols to protect your system.**
6. **Implement the security features provided by device and system vendors.**
7. **Establish strong controls over any medium that is used as a backdoor into the SCADA network.**
8. **Implement internal and external intrusion detection systems and establish 24-hour-a-day incident monitoring.**
9. **Perform technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns.**
10. **Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security.**
11. **Establish a SCADA "Red Teams" to identify and evaluate possible attack scenarios.**
12. **Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users.**
13. **Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection.**
14. **Establish a rigorous, ongoing risk management process.**
15. **Establish a network protection strategy based on the principle of defense-in-depth.**
16. **Clearly identify cyber security requirements.**
17. **Establish effective configuration management process.**
18. **Conduct routine self-assessments.**
19. **Establish system backups and disaster recovery plans.**
20. **Senior organizational leadership should establish expectations for cyber security performance**

and hold individuals accountable for their performance.

21. **Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.**

RECOMMENDATIONS

As companies utilizing SCADA and ICS begin to move toward a more cyber security aware practice, there will be questions of where to begin. First and foremost, businesses will need to find their points of weakness. This can be done with an initial assessment and something known as a Gap Analysis. A Gap Analysis identifies where you stand both from a policy and a technology stand-point.

Next, businesses will need to put into place a plan of action to implement changes and improvements both in policy and with technology. The plan of action may seem daunting, but changes can be segmented and budgeted to become more manageable. Realistic dates should be set based on priority and cost.

The biggest change starts with practices. Policies and training should be put in place to ensure all departments and employees play their role in becoming more security aware. One of the most common attacks against any company is social engineering

CONCLUSION

With the changes that have been required in finance and in government contracts, it is time for SCADA and ICS to move toward a more secure stance in the cyber space. The changes may seem overwhelming for any IT security staff, but a push in this direction will prevent disasters from occurring in the future. With the world moving closer and closer to cyber integration, cybersecurity will become more and more important. It is best to be proactive on these changes rather than reactive as breaches in some key industries could come at the cost of human lives.

H2L Solutions prides itself on helping organizations become compliant with cybersecurity regulations and standards. If your organization has any questions concerning the regulations or standards for ICS and SCADA systems, please contact us at info@h2lsolutions.com.

REFERENCES

1. NIST-800 82 - https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
2. ICS Cyber Security Conference - http://www.icscybersecurityconference.com/ust-vulnerable-industrial-control-systems-learned-ics-attacks-2016/
3. Department of Energy 21 steps to improve security on SCADA Networks - https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf
4. The 62443 Series of Standards - http://isa99.isa.org/Public/Information/The-62443-Series-Overview.pdf