**What is the SCADA System in Cybersecurity**

            Supervisory control and data acquisition (SCADA) are the infrastructure processes that help run many different systems that help us get through our day-to-day lives. Processes such as water treatment and gas pipelines fall into this system, and space stations and power generation companies also fall into this infrastructure. Through this system, the people working can coordinate the processes needed in real-time to help these processes work. However, one may ask how it works, what are its potential weaknesses and how one mitigates or erases these risks.

*What is the SCADA system?*

          One thing that should be known about this system is that for the most part, it requires human input for any of the plans in the system to work. Throughout every article, the most used factor is the Human machine interface (HMI) which is how the person can interact with the system process that is being used. With that being one article states that the SCADA system is “A SCADA system is a combination of hardware and software that enables industrial process automation by capturing Operational Technology (OT) real-time data. SCADA connects the sensors that monitor equipment like motors, pumps, and valves to an onsite or remote server.”(Wangsness,2024). Systems supported by this can be as small as traffic light control systems or as big as water distribution plants. With how fast we are advancing as a society they have even been used in the exploration of space, these systems are just scratching the surface of how much we rely on the SCADA system. Breaking this down what needs to be taken away is that this system is basically a second brain a human can use to make sure processes are being run smoothly. This system works by examining a system and if it were to mess up this system would be able to detect it almost immediately and prepare a repair plan for how to get things back up in running. This helping to maintain upkeep and easy integration whenever a person is needed for repair.

*Vulnerabilities within the system*

          With how easy this system is when it comes to getting processes done, there sadly arises the risk of cyberterrorism attacks. Most people seem to believe that these systems are secure on the physical side since the physical servers and human-machine interfaces are kept safely locked up away from attack. However, what most seem to forget is the software side of the scada system which is always under the threat of a breach in security. In one article they date the first software breach back to 1982 in Siberia quoting “The Siberian pipeline explosion in 1982 is believed to be the first cyber incident in the history of SCADA systems” (Ismailetal,2014). This was done when a user put a Trojan horse virus into the SCADA system which changed the operations of the valves and pumps of the pipeline. This led to an increase in gas pressure that went above the capabilities of the pipeline which led to the explosion. Later in 1994 another user was able to breach the Salt River project through a dial-up modem and was able to modify the log files within the computer system. These attacks are just a glimpse of how long these SCADA system software vulnerabilities have been present in the world. One threat thrown around is the security protocols or lack of protocols when packets in a system are being sent. When someone sends a packet they are in control of where it goes and how it is used and sadly in some cases the packet will be misused when it is sent. However, one common theme in all these attacks is the human factor present in each of them. Somehow each hacker was able to gain access through unknown means in a lot of them with others gaining access from the employees that work on these projects. Recently, we learned in class how another vulnerability with these systems is how old the machine systems are in some areas there is a chance for easier attacks. Because, of their age a lot of their software could be left behind which then leads to a easier means of breaking through the act of taking advantage of older software. However, this shows how the SCADA system's greatest threat is human interaction which for the most part is the hardest to combat.

*Recommended Improvements to the SCADA System*

          From the articles read it is obvious there are improvements to the SCADA system needed moving forward. Software protection would be a great start in the improvement of security whether it be through more encryption of the code or constant checking of the digital packets being sent and received. Having a cyber security team for these things would create a better security force in helping ensure that mitigation of risk is constantly present within the SCADA system. However, this comes with the funding and employees needed to make sure these security protocols are being upheld. Sadly, human error is present with everyone so even if the funding was present there is always the risk of a person making a mistake when it comes to the security reviews proposed for the software. Leading to the main change that needs to be made is the human factor within this system. This task sadly is nearly impossible since no one is perfect but there are still a few things that can be done to improve human factors. Proper background checks are a great start as many of the potential employee’s present could be hacktivists in disguise trying to gain access to the system in hopes of making a grand display through any means. Next, there could be the training being done brought into question, if the people hired were to receive vigorous training there could be a decrease in threats since malicious code and possible weaknesses could be noticed by these employees. Lastly for good measure could be a daily review of these systems and what was done with them on the day an attack was brought up. While this happens at some places ensuring that a regular check of the system is in place would be a great start in improving the security measures of the SCADA system.

*Conclusion*

          The SCADA system is an amazing invention that is used daily in the day-to-day lives of any person who walks the earth. Learning how it works shows how much we rely on the processes that are performed within the system. Sadly, due to how good this system is a lot of targets have been placed on it. While every day the threat of these attacks rises so do the people who will fight back and mitigate these threats from happening to help ensure that the security is up to date. One day even the human mistakes made can be erased which will allow the SCADA system to truly shine all we need is a little more training and understanding to make this system at its best.

*Sources*

Wangsness, C. (2024, September 20). What is a SCADA system and how does it work?. Embedded Industrial Computers for Edge & IoT. https://www.onlogic.com/blog/what-is-a-scada-system-and-how-does-it-work/

Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2022a, November 25). SCADA vulnerabilities and attacks: A review of the state‐of‐the‐art and open issues. Computers & Security. https://www.sciencedirect.com/science/article/pii/S0167404822004205