Write Up-SCADA

Leyah Knox

Supervisory Control and Data Acquisition (SCADA) systems are vital to organizations as they allow them to manage and monitor important infrastructures including but not limited to electricity, water, transportation, manufacturing, and other types of industrial services. Organizations are able to gather information from equipment and make modifications to operation methods through a single location through SCADA systems.

While the connectivity of SCADA systems to networks and technology does allow organizations to gain greater control over their operations, it also exposes them to potential cyber security risks. Cyber attacks on SCADA systems can result in equipment failure, disruption of service, loss of revenue, and potentially endanger public safety. Organizations can mitigate these risks through utilization of network security, access control, monitoring, updating of systems, employee education regarding cyber security, and development of disaster recovery plans and backup procedures. Supervisory Control and Data Acquisition (SCADA) systems are industrial control systems utilized by organizations to manage equipment and processes. Organizations utilize SCADA systems to gather data from sensors and other devices and send that data back to a central system where employees can observe the status of processes. Employees can utilize SCADA systems to modify processes when necessary. SCADA systems provide value to organizations as many industries cannot afford to rely solely on employees physically inspecting each piece of equipment or process at all times. SCADA systems enable employees to view data in real-time and react quickly to issues. The National Institute of Standards and Technology describes industrial control systems, which include SCADA systems, as used to manage physical

processes and possess unique requirements related to reliability, safety and performance. This means that a malfunction of a SCADA system can impact physical equipment and actual operational processes. Many industries employ SCADA systems. An excellent example would be the energy industry. Electric utilities can utilize industrial control systems to manage and monitor portions of the power grid. SCADA systems can assist organizations in managing electricity generation, transmission and distribution. NIST states that industrial control systems are crucial to the energy sector and are utilized in order to facilitate power generation, transmission and distribution (McCarthy et al, 2018).

In addition to the energy sector, SCADA systems are employed within the water and wastewater sectors. Water treatment facilities can employ SCADA systems to manage pumps, water levels, pressures and other equipment. If an issue arises, employees can utilize the information provided by the SCADA system to react. Manufacturing organizations can also utilize SCADA systems to manage production equipment and manage industrial processes. Other industries employing industrial control systems include oil and gas, chemicals manufacturing, food and beverages manufacturing, pharmaceutical manufacturing, and transportation. Employment of SCADA systems can enhance efficiency for these organizations as employees can manage multiple aspects of operations from a single location.

However, this also implies that a malfunction of a SCADA system can impact numerous aspects of an organization at once. One of the primary vulnerabilities associated with SCADA systems is that many systems were not originally designed with contemporary cybersecurity threats in mind. Most industrial systems were designed to prioritize reliability and ensuring continuous operation. As technology progressed, some SCADA systems were linked to organizational networks and other systems. Linking SCADA systems to organizational networks

provided them with increased communication capabilities but also exposed them to additional vulnerabilities to attack. NIST identifies several vulnerabilities and threats that exist within industrial control systems including inadequate security controls, network vulnerabilities, and complications arising from linking control systems to other networks. Should an attacker gain entry into a SCADA environment, they may be capable of disrupting control systems managing physical processes. A second significant vulnerability is obsolete software and hardware. Many industrial systems are challenging to upgrade as upgrading requires taking the systems offline which may disrupt vital services.

Therefore, many organizations continue utilizing outdated software or hardware that may contain known security flaws. NIST has emphasized the significance of identifying, monitoring, and managing operational technology assets as vulnerabilities in these systems can create avenues for cyber attacks. Poor access control can similarly present complications. Should excessive employees possess access to critical SCADA systems, an attacker obtaining access to one employee's account may potentially access systems they should not be permitted to control. Employing strong passwords, multifactor authentication, least privilege access, and effective account management can assist in mitigating this vulnerability. A cyber attack on a SCADA system can produce effects beyond merely affecting computers and data. Since SCADA systems can control physical processes, a cyber attack on a SCADA system could cause physical equipment to operate improperly, cease operating entirely, or become inaccessible. For instance, a cyber attack on an electric utility could disrupt power generation or distribution. Such disruptions could result in blackouts affecting residences, businesses, hospitals, schools and other organizations. A cyber attack on a water treatment facility could disrupt pump operations or

treatment processes. A cyber attack on a manufacturing facility could halt production causing financial losses for the manufacturer.

Additionally, effects resulting from a cyber attack on a SCADA system can extend beyond the organization directly targeted by the attack. Critical infrastructure systems are connected to daily life therefore, disruptions can impact large populations. NIST has stated that cyber attacks on industrial control systems in domains including energy, water, and chemical facilities can result in risks related to public health, safety and environmental concerns. The SCADA system testbed research conducted by authors of the MDPI article also illustrates why cybersecurity testing is essential. SCADA testbeds allow researchers to study attacks and cybersecurity defense strategies without placing actual critical infrastructure at risk (Moraes et al, 2018). Such research can aid organizations in understanding vulnerabilities prior to attackers exploiting those vulnerabilities. Organizations can take various measures to improve security posture of SCADA systems. One essential approach is network segmentation. Rather than connecting SCADA networks directly to all other networks, organizations can isolate critical operational systems from standard business systems. Isolating critical operational systems from standard business systems makes it harder for an attacker to migrate from one compromised system to another. Organizations should also implement strict access controls. Employees should only have access to resources required for completing their job functions. Strong passwords, multi-factor authentication, account monitoring, and periodic reviews of user authorizations can assist in preventing unauthorized access.

Another important measure organizations can take is updating equipment software when it can be done safely. Organizations should consistently identify vulnerabilities and determine which systems require security updates. Since many SCADA devices cannot be safely taken

offline for upgrades, organizations may require utilizing alternative security measures such as network monitoring or supplementary protective equipment when immediate patching is not feasible. Monitoring is equally important. Organizations should monitor SCADA networks for irregular activities and investigate suspicious behaviors. An incident response plan can provide employees with guidance on how to react if an attack occurs. Organizations should also establish backup plans and recovery plans so that they can recover critical systems after an incident. NIST recommends security controls that recognize unique performance requirements of industrial control systems. Employee training should also be considered as employees require knowledge regarding cybersecurity threats such as phishing,stolen credentials, and unauthorized access. Technical security controls can be rendered less effective if employees lack awareness and knowledge on how to report suspicious activity.

REFERENCES (Extra)

1. Teixeira, M., Salman, T., Zolanvari, M., Jain, R., Meskin, N., & Samaka, M. (2018). SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach. *Future Internet*, *10*(8), 76. https://doi.org/10.3390/fi10080076