CALIFORNIA RURAL WATER ASSOCIATION
MEMBERGUARD
Serviced by Glatfelter Public Practice

RISK COMMUNIQUÉ

A technical reference bulletin by the Risk Control Services Department of the Glatfelter Insurance Group

SCADA Network Security

The following guidance is for public and private entities that are responsible for providing critical services such as water supplies, waste water treatment, electrical power distribution, natural gas, and transportation that rely upon computer controls to monitor system performance and security. The U.S. Department of Energy in conjunction with the President's Critical Infrastructure Protection Board, published, "21 Steps to Improve Cyber Security of SCADA Networks.", and portions of this text are included below.

SCADA

Supervisory control and data acquisition (SCADA) networks contain computers and applications that perform key functions in providing essential services and commodities (e.g., electricity, natural gas, gasoline, water, waste treatment, transportation) to all Americans. As such, they are part of the nation's critical infrastructure and require protection from a variety of threats that exist in cyber space today. By allowing the collection and analysis of data and control of equipment such as pumps and valves from remote locations, SCADA networks provide great efficiency and are widely used. However, they also present a security risk. SCADA networks were initially designed to maximize functionality, with little attention paid to security. As a result, performance, reliability, flexibility and safety of SCADA systems are robust, while the security of these systems is often weak. This makes some SCADA networks potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could result in public safety concerns and/or serious disruptions to the nation's critical infrastructure. Action is required by all organizations, government or commercial, to secure their SCADA networks as part of the effort to adequately protect the nation's critical infrastructure.

The President's Critical Infrastructure Protection Board, and the Department of Energy, have developed the steps outlined here to help any organization improve the security of its SCADA networks. These steps are not meant to be prescriptive or all-inclusive. However, they do address essential actions to be taken to improve the protection of SCADA networks. The steps are divided into two categories: specific actions to improve implementation, and actions to establish essential underlying management processes and policies.

21 Steps to Improve Cyber Security of SCADA Network:

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.

This is a sample guideline furnished to you by MemberGuard. Your organization should review it and make the necessary modifications to meet the needs of your organization. The intent of this guideline is to assist you in reducing risk exposure to the public, personnel and property. For additional information on this topic, you may contact your Risk Control Representative. www.MyMemberGuard.com

© 2016 MemberGuard. All Rights Reserved

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 concerns.
10. Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security.
11. Establish 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 processes.
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.

This is a sample guideline furnished to you by MemberGuard. Your organization should review it and make the necessary modifications to meet the needs of your organization. The intent of this guideline is to assist you in reducing risk exposure to the public, personnel and property. For additional information on this topic, you may contact your Risk Control Representative. www.MyMemberGuard.com

© 2016 MemberGuard. All Rights Reserved