SCADA Worm

Student’s Name

Institution

**Introduction**

Supervisory Control and Data Acquisition (SCADA) system utilized for controlling and monitoring geographical remote operations. It is used to have control of the system behind the scene to ensure that a function is completed efficiently. It collects operational data and sensor measurement from the field and then process display and relay information across the field to the control command so that the data could be utilized. According to (Mackenzie & Peter, 2012), the average citizens are not aware of SCADA and its importance to the operations of various sectors. The SCADA system are used to control some of the vital infrastructure such as energy, oil and gas, nuclear facilities and water treatment plants and therefore, it is an essential aspect for any control. This paper therefore, provides a detail illustration of the impact of vulnerability of the SCADA Worm on the critical United States’ infrastructure; describe the methods to mitigate the vulnerabilities, as they relate to the seven (7) domains. It also Assess the levels of responsibility between government agencies and the private sector for mitigating threats and vulnerabilities to our critical infrastructure. It finally, Assess the elements of an effective IT Security Policy Framework, and how these elements, if properly implemented, could prevent or mitigate and attack similar to the SCADA / Stuxnet Worm.

**Impact of SCADA and Stuxnet Worm**

The SCADA and Stuxnet Worm have critical impact on the infrastructure in the United States. The fact that SCADA and Stuxnet can have access to critical infrastructure it exposes the United States, critical infrastructure to cyber attack. The fact that SCADA does not require human control makes it more vulnerable to attack and therefore, SCADA and Stuxnet Worm exposed the United States’ infrastructure to external attack. (Harrison, 2018). A study conducted by Harrison (2018) on vulnerability of system concluded that with knowledge of SCADA any individual can access SCADA software and crate back entry, and this could increase chances of attack to the system. Therefore, the SCADA and Stuxnet Worm make the critical infrastructure in the United States, more vulnerable to attack by cybercrimes and other people or enemies and therefore, it can cause the United States lose of vital information to enemies hence could compromise the national security (Kaplan, 2017). The cyber attack to critical infrastructure will definitely increase due to SCADA and Stuxnet Worm.

**Methods to mitigate vulnerability as they relate to the seven domains**

The domains are critical point to access an entry into a system. The seven domains are workstation, remote access, LAN to WAN Domain, WAN domain and system application domain. These domains are critical for efficient and secure operation for any business. The vulnerability around these domains can create access, which permit cyber attack hence can cause serious damage to an organization (Mackenzie & Peter, 2012). Therefore, the access must be regulated through passwords, codes and policies. In workstation, a strong authorization password must be configured to ensure that only authorized person can have access to the station. The LAN and WAN system also require three level encryption configuration to filter in and outgoing messages. It therefore, important for a business to protect each of these seven domains from an attacker from get easy access to the private data.

**Levels of responsibility between government agencies and the private sector for mitigating threats and vulnerabilities to our critical infrastructure**

The government and the private sector have shared responsibilities to ensure that IT infrastructures are protected. The government has responsibilities to come with policies, which can ensure that infrastructures are protected from access. The corporate world design the best methods needed to protect the infrastructure and conduct research to develop some of the latest techniques, which can be utilized to reduce the vulnerability of IT infrastructure. For example, the U.S. government has enacted data private laws to limit access to private. According to (Kaplan, 2017), the government plays a critical role in maintaining the law and order, and therefore, it punishes individuals who have are found guilty to have violated the law to create vulnerability to the system. The private sector and the government also share information related to vulnerabilities including threats in the system and develop critical applications or methods, which can be used to address the problem. Therefore, the government and the private sector work together to assess and address the issues related to vulnerability to the IT infrastructure in the country.

**Elements of an effective IT Security Policy Framework**

Effective IT Security policy framework is an important component of protecting vital IT system. There are several policies, which have been enacted by the government to address the issue of vulnerabilities. The government through partnership with stakeholders have established National Institute Standard and technology (NIST), National Security Agency (NSA), the office of Management and Budget (OMB) and the National Security Agency (NSA and the General Accounting Office to address the issues related to vulnerability to improve the security system of key infrastructure in the country (Lewis, 2018). These five bodies periodically assess the documents and security level of the every key infrastructure to make sure that any vulnerability is detected early to prevent any attack to the system. These agencies also analyze the depth of threats and issue set rules and guidelines to provide much impact to the economy and to avoid any future attack to the systems.

# References

Harrison, S. (2018). Attack Code for SCADA Vulnerabilities Released Online. *International Journal of Information System* *, 21* (5), 2-15.

Kaplan, D. (2017). Defend Your Industrial Control Systems: 8 Practical Steps. *International Journal of Information and Business Security* , 12-38.

Lewis, N. (2018). What does the Stuxnet worm mean for SCADA systems security? *Information Security and Business ethics* *, 12* (8), 2-35.

Mackenzie, H., & Peter, M. (2012). Cyber Attacks on U.S. Critical Infrastructure will Intensify. *Journal of information System and Security* *, 21* (8), 2-34.