Scada worm term paper examples

Law, Security

\n[toc title="Table of Contents"]\n

\n \t

1. Introduction \n \t
2. Vulnerabilities \n \t
3. Mitigation \n \t
4. Levels of responsibility \n \t
5. IT framework \n \t
6. References \n

\n[/toc]\n \n

Introduction

Supervisory Control and Data Acquisition (SCADA) systems are computer programs which are used in monitoring and controlling operations which are remotely located. The process of monitoring is unknown to those who are undertaking the operations. This is becoming a problem to governments, individuals and private practitioners. This is because with these silent operations, there is a possibility of obtaining private and confidential information regarding employees. There is also the possibility of interrupting with operations. SCADA systems are known to control some vital and critical infrastructure which is found in industrial settings. The range of the industries includes oil and gas to nuclear sectors. Critical infrastructure is the IT assets and networks which if they are interrupted will cause enormous losses on health, security, and the economic status of individuals and also will disrupt the efficient working of any government(Hildick-Smith, 2005).

Vulnerabilities

The SCADA worm is vulnerable. One of the reasons for this is that with the connectivity that SCADA worm has on several networks, this raises security concerns for the networks which are connected. If the SCADA worm network is not secured properly, this will mean that the connectivity and the security of the enterprise networks will be vulnerable to attacks. The integration of the control systems and that of the enterprise networks is vulnerable to attacks. Many organizations have connected their systems with SCADA networks. If there are no secure remote connections for remote SCADA networks, this will mean that the networks are vulnerable to attacks. There should be measures taken to ensure that the remote connections are as secure as possible. With SCADA worm, the systems that it monitors could be insecure if the remote connections that it has is not well maintained and secured(Ericsson, 2010).

Another vulnerability that comes with SCADA worm is that it attacks systems that use standardized technologies. The attack it is reported to have undertaken in Iran is because the systems in Iran made use of Windows Operating systems. The programmers of SCADA worm understood well how windows could be attacked. This is a vulnerability that SCADA worm and all control systems have(Creery & Byres, 2005).

Another vulnerability of SCADA worm is that there is public availability of technical information regarding the control of control systems. With this availability of this critical information, it is easier for attackers to get access to the systems which are being attacked. There are holes which are poked to the new integration of the connectivity. With the SCADA worm, many

computer systems can be accessed by attackers which are a serious security concern(Ralston, Graham, & Hieb, 2007).

Mitigation

There are various mitigation strategies that can be used to protect control systems. One of the mitigation strategies is to have users have authenticated. This is in relation to user domain of the seven domains of IT infrastructure. Users should be trained to secure their domains and computer profiles. This way, they will protect the attackers from entering into the systems(Hildick-Smith, 2005).

Another mitigation strategy that can be engaged is to have the workstation domains authenticated with secure systems. The scripts should be signed before they are allowed to run on the workstation computers. The workstation domains are the places where the processes are run. There is a need to secure these domains. This way, the workstation domain is protected from attacks.

The LAN should be protected so that it is safe. The LAN should be set so that it operates under a firewall. This way, all attacks will be locked outside the domains. The SCADA worm will be vetted before being allowed to get to the LAN. This way, the LAN will be safe(Ralston et al., 2007).

FTP servers should be protected so that they do not download or upload illegal software. The DOA attacks will be eradicated with the use of DMZ zone and the use of a firewall. This will protect the WAN from attacks.

Another domain is that of LAN/WAN. There should be boundaries put in place to protect the LAN and WAN interconnection. This will enable the connections between these two networks. Another domain that should be protected in

control systems is that user application domain. The database and user access servers should be protected. The mitigation that could be undertaken in this domain is that of ensuring that the users are authenticated(Munro, 2008).

Levels of responsibility

The government and the private sector should be involved in undertaking the mitigation of SCADA control systems. The current responsibility of the process of mitigation is that each sector tries to undertake their own security measures. The private sector secures their own networks and systems while the government secures the national networks. It can be said that the government does the overall networks and it has been seen to help the private sector to protect the attacks. At this point, the two sectors are doing all they can to have secure systems in place.

IT framework

One of the security frameworks that can be implemented for effective and reliable security in the SCADA worm attack is that of NIST SP 800 53. The implementation of NIST SP 800 53 will facilitate the development, dissemination and update of formalized access policies and other procedures that gather for the management and coordination of the system. The Act stipulates the effective methods for account management, access enforcement, control of information flow, duty separation and least privileges. It will also manage other factors such as session controls, automatic marking, and management of publicly-accessible content, user-based collaboration and access control. The guidelines apply to specific and

general use with clear implications on the system security status, forensic audit quality and effective controls(Ralston et al., 2007).

References

Creery, A., & Byres, E. (2005). Industrial cybersecurity for power system and SCADA networks. Petroleum and Chemical Industry .

Ericsson, G. (2010). Cyber security and power system communication—essential parts of a smart grid infrastructure. Power Delivery, IEEE Transactions on.

Hildick-Smith, A. (2005). Security for critical infrastructure scada systems. SANS Reading Room, GSEC Practical Assignment, .

Munro, K. (2008). SCADA–A critical situation. Network Security.

Ralston, P., Graham, J., & Hieb, J. (2007). Cyber security risk assessment for SCADA and DCS networks. ISA transactions.