Cyber security case study: pure land wastewater treatment

Introduction

Every organization should use the industrial control system to ensure the success of their departments and ensure the ultimate success of critical operations within the premise. Since such organizations will rely on the services of these agencies, it is necessary to have the right strategies in place that will result in the security of such information. The contemporary society entails handling of large volumes of data. Therefore, there is a need for the use of a sophisticated system that will improve key departments and shorten the time taken in controlling key instances within the departments. It is never possible to employ the manual processes in the execution of critical cases within current organizations. Ideally, the system is essential since it controls some processes within the organization. Some of the processes include electrical power generation as well as distribution, manufacturing, sewerage management among other processes that are relevant to the entire process. Water management should be the responsibility of every stakeholder in an economy since it contributes to the health of individuals in different parts of the world. The instances that relate to PureLand treatment plant inclines with the main of these cases since it employs the industrial control system in managing some processes. However, the company did not follow all the stipulated laws, and that resulted in the conflict that emerged between the company and the Department of Homeland Security. The issue in the process was a lack of the most appropriate system that protected the ICS against cyber security threats and vulnerabilities. The use of dangerous chemicals during water treatment is also an instance that affected the success of various departments within the organization. DHS did the most

extensive research and identified that the company lacks the necessary approaches to protecting their information. Therefore, it’s hard to protect the trade secrets while handling most operations within the premise. The process seems complicated, and the company found it is prudent to outline all the necessary steps that will ensure the success of the primary instances that relates to the situation within the environment.

One approach that made the entire process possible was the examination of the computer system. It is evident that the company utilized the system in sterilizing and that employed the use of toxic chemicals, and such remains one of the critical sources of information that will help in the process. The computer system is an important part of every organization since they store all the vital information that relates to critical operations within the organization. Ideally, there is need to provide a robust cyber security in the process. That will have control on the access priorities and improves the manner in which the premise will handle chemicals during the execution ok fundamental processes. There is need to have only the right stakeholders that will have access to sensitive data about the organization. That will make it possible to eliminate any instance of threat that might affect the success of critical operations within the organization.

The existence of the Department of Homeland Security is a crucial component in any given community and takes the lead in regulating all the industries of ICS. Additionally, it provides the specific regulation that contributes to the success of critical operations within the premise. Even though the pure land industry has one of the standing track records, it is evident that it still fails in some instances and it is necessary to employ the

most effective approaches that will result in the complete success in the major areas. The integration of DHS in the whole process is also essential since it will provide the necessary tools and techniques that ensure efficient operation within the organization. That will result in the ultimate success of key departments within the industry.

The Security Status of the System

It is evident that Pure Land lacks the most sophisticated approach that will enable it to handle the number of security concerns that are likely to result in the failure of key departments within the premise. There is need to have these processes in place to protect their information, data as well as chemicals. That is key since it will prevent any malicious activity that might hurt the success of key departments within the industry. The ability of less sophisticated system is a leeway for the attackers who are likely to sabotage the existing chemicals and that contributes to the increase in contamination. The process is detrimental to the organization as well as the health of other stakeholders in the environment. Ideally, that is the case since it will affect the reputation of the company. Additionally, it will result in te production of contaminated water that will have an adverse impact on the health of stakeholders in different parts of the world. Cyber security is sensitive, and companies must employ both the logical as well as physical protective methods to ensure the confidentiality as well as the integrity of most of their information. The company lacks the integration of key approaches such as antivirus, firewalls among other logical measures that will ensure the success of the entire process. Again, the company does not have a suitable asset tracking as well as a management system and that makes it difficult to have

control on the primary instances within the premise. The best option is for DHA as well as Pureland to address all these situations to embrace their operation in the region.

Overview of the Network Topology

The effective communication among all the lines within the premise contributes to its success in some instances. There is the existence of a backbone cable that moves through all the sections and offers all the information that stakeholders might find useful in the entire system. Ideally, the depiction represents a ring topology since there is a close contact between different nodes in the system. Additionally, it is evident that there is a connection of one node to two others in the system and that plays a crucial role in the relay of vital information that relates to the entire communication process within the system. The limitation of the topology is the ability to introduce the aspect of single point of failure that might affect critical operations within the network (Shaker & Reeves, 2005). Sending a packet through the system makes it pass through all the other nodes till the destination. Therefore, a failure of one node can result in the ultimate failure of the entire system, and that should never be the same in an efficient system.

Figure 1: PureLand Network Diagram

Weaknesses in the Design

The company’s website is never safe, and that is due to the number of weaknesses in the system. First, the entire system has one firewall and that

compromise the security in the major departments. Since it lies at the front of the router, it is never effective, and it is necessary to have the right approaches in place that will embrace the security of the system. The system might find it difficult to filter and block any malicious software in the system. There is need to have at least two firewalls that will contribute to the success of critical operations within the organization. That should exist behind the router as well as in front of the router to offer the most efficient security to critical operations within the system. Again, it is evident that the company lacks the proper protection of their systems such as their server and that might also contribute to the failure of key instances within the process.

Associated Improvements

The ICS is never sufficient, and the company can implement some approaches that will help the success of the system. The aim should be the formation of a system that meets the needs of stakeholders in different departments. The first process should change the network topology since it is likely to result in the failure of key agencies within the industry. Therefore, there is need to implement the start topology since it will cater to the needs of various stakeholders within the system and that will result in the success of critical operations within the industry. Apart from the relevant security measures, the existence of physical security measures will also improve the success of critical operations within the premise and that key in meeting the mission as well as the vision of the company. Having enough security measures in place should be the role of the management before embarking on the actual implementation of the physical components of the system.

Additionally, there is the need of having internal firewalls on top of the external firewalls to embrace success in the entire system. The main aim of the process is to filter any traffic that will emerge in the process. The result will be the existence of improved communication that will enhance service delivery among different departments within the premise.

Threats and Vulnerabilities Facing Industrial Control Systems

Threats

The industrial controls system is never safe and suffers from some threats. Therefore, there is need to implement the best approaches that will restore security to the information since that will have a positive impact on the ultimate success of critical operations within the premise. There are some threats that are likely to affect the success of the system. Some of them include equipment failure, external attackers, terrorist groups as well as unfortunate events among others. All these components will have an adverse impact on the success of key elements of the organization, and there is need to have the right approaches that will restore security in the system and ensure the success of key departments within the industry. The treats can form part of either the external or internal threats. The internal threats relate to the personnel within the premise and might result in data leakage as well as the actual damage to the information system. Therefore, there is need to have the right approaches that will ensure accountability of critical processes. The external threats may include viruses, malware as well as hackers among others. It is the role of the management to implement the best approaches that will contribute to the success of key departments

within the organization and improve the quality of service. That will ensure sustainability and also embrace the reputation of the industry, which is critical in providing a competitive advantage in the global market.

Vulnerabilities

The vulnerabilities to the ICS frameworks can be partitioned into three general gatherings including a stage; handle and procedural, and arrange vulnerabilities.

Platform Vulnerabilities

The stage vulnerabilities may incorporate equipment, programming steps, setup, and stage malware insurance vulnerabilities. The absence of proper support of the presence of poor designs on a hierarchical stage may prompt to simplicity of digital assaults (Knapp, 2011). As far as stage programming vulnerabilities, the absence of programming patches may make an ICS framework is powerless against aggression. The databases may likewise acquaint defenselessness do with the capacity of an aggressor to execute SQL infusions. As far as stage equipment vulnerabilities, an ICS framework may have ineffectual testing of the security changes or the absence of test offices. As far as malware vulnerabilities of ICS stages, the lack of antimalware programming establishments may make the ICS helpless against assault (Peng et al., 2012). That will like this bring about poor execution, framework alterations that may antagonistically affect the frame, information erasure, and the loss of context accessibility.

Procedures and Policy vulnerabilities

The procedural and strategy vulnerabilities include the absence of sufficient and appropriate strategies and methodology for securing the ICS and together frameworks associated with it. Security arrangements and techniques oversee the way workers and all partners ought to deal with data and different resources in an organization. That can be conceivable because of the absence of coordination between the administration and the security workforce or the absence of satisfactory abilities for the security faculty.

Network Vulnerabilities

The setups on the system can make the system helpless against assaults particularly when those designs are not appropriately executed. Something else is the calculations utilized as a part of the system of network offices. For example, the hashing calculation that is employed as the necessary standard for verifying API is helpless to crashes. It permits the aggressors to assault a system using beast constrain assaults. Likewise, the absence of border safety efforts may open the ICS system to digital attacks. The system may need firewalls, or it might ineffectively design the ones that are there, in this manner bringing about the passage of redundant information to the LAN (Weiss, 2010).

Advanced Persistent Attacks

Progressed Persistent Threats can be said to be focused on assaults that different utilization strategies, for example, spam, SQL infusion, and phishing among others to pick up the passage into a framework. Of later, the focused on assaults and progressed determined assaults have been exceptionally predominant creating significant information spillage and misfortune to

interlopers. The progression of innovation has energized many aggressors that are currently utilizing advanced programming to target specific organizations with a point of harming poor taking classified information (Weiss, 2010). The security groups of organizations ought to know about these assaults and set up the proper safety efforts to protect the ICS against these assaults.

Applicable Regulations and Compliance

I. There are security strategies and method rules in NIST SP 800-12, and that can be available in (Stouffer et al., 2011).

II. The NIST 800-53 is likewise other security rules for system borders and additionally the product for an ICS organize.

III. The other relevant direction is NIST 800-82 that involves the proposals for protection inside and out for the system offices and ICS.

IV. The RBPS Metrics 8. 2. 5 additionally contains directions for ensuring passwords and through and through basic data utilizing suitable techniques and methods like validation.

V. The ISO/IEC 27001-27005 additionally contains rules for the components required in an observing framework.

VI. The other control is contained in NIST SP 800-41. The direction offers the rules for the best approach to utilize the firewall and the distinctive sort of firewalls including a depiction of where each is appropriate.

VII. The rules for the security of the interruption counteractive action/identifying frameworks are found in NIST SP 800-91.

The Desired Future State of ICS Security

Pure land ought to need to put a firewall, and a switch between the corporate system and the control organize. The organization needs a resistance inside and out a methodology for securing its ICS framework and the various frameworks that associate with this framework. A safeguard inside and out framework gives a security execution that makes it hard for the aggressors to experience (FISMA, 2005). The utilization of security frameworks and gadgets from various sellers can make the digital security of pure land to be as far reaching as it is wanted. The guard inside and out security utilizes different layers of security on the system consequently making it practically incomprehensible for aggressors to hack into the framework.

The other wanted condition of Pure Land’s ICS security is to have every one of the partners in charge of the safety of the ICS structure. The organization ought to prepare every one of the clients and laborers on the security issues and make them be in charge of the safety of the structure. The security workforce and the IT faculty ought to likewise be altogether prepared about the safety necessities for the ICS framework with the goal that they can be able to create legitimate security approaches and systems for the ICS arrange.

The other sought future state for Pure Land’s system is to have a Demilitarized zone that partitions the corporate system, and the control

arrange. That DMZ needs to contain basic segments, for example, the information antiquarian, the remote get to focused, and the outsider gets to focuses (Macaulay et al., 2011). Directly, pure land has the information antiquarian that is not appropriately shielded from digital assaults. Pure land should have its firewall offering three interfaces instead of the typical ones that are: open and private. The primary interface needs to set up an association with the corporate system, the second one to build up an association with the control organize while the third ought to set up an association with the system shared gadgets like the information history specialist.

The major test before the pure land Industrial Control System is, they should diminish the Cyber security episodes and even should move their emphasis on taking wellbeing measures to kill the physical Incidents while working with those hazardous chemicals. Another test is that the pure land Securities must procure IT staff and security examiner to be consistent with the CFATS – Chemical Facility Anti-Terrorism Standards directions as managed by the Department of Homeland Security (DHS).

The special difficulties that exist in securing the Pure Land Industrial Control System are, security control apply in business PC frameworks can’t be connected in Industrial Control Systems, and Industrial Control frameworks are assembled utilizing legacy gadgets, running legacy conventions to work in the routable system can challenge.

Conclusion

Pure land discovers them in an express that obliges them to move quickly and make a move in regards to the digital security of their ICS framework. The case demonstrates that DHS distinguished many issues and gave the organization a particular period for tending to every one of those issues if their frameworks must be protected from digital assaults. The paper has highlighted each one of those issues and built up an arrangement on how pure land ought to go to ensure that it has a tight security for the ICS and the general corporate system.

References

FISMA (2002). Federal Information Security Management Act of 2002, Section 301: Information Security, http://csrc. nist. gov/drivers/documents/FISMA-final. pdf

Kirby, C. (2003). Forum focuses on cybersecurity. San Francisco Chronicle.

Knapp, E. (2011). Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Waltham, Massachusetts: Syngress.

Macaulay, T., Bryan, L. & Singer, L. (2011). Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS. CRC Press, London: NY.

Peng, Y., Jiang, C., Xie, F., Dai, Z., Xiong, Q., & Gao, Y. (2012). Industrial control system cybersecurity research. *Journal of Tsinghua University Science and Technology* , 4(10), 1396-1408.

Shaker, A., & Reeves, D. S. (2005, August). Self-stabilizing structured ring topology p2p systems. In *Peer-to-Peer Computing, 2005. P2P 2005. Fifth IEEE International Conference on* (pp. 39-46). IEEE.

Stouffer, K., Falco, J. &Scarfone, K. (2011). Recommendation of the National Institute of Standards and Technology. Special Publication 800-82. Retrieved from http://csrc. nist. gov/publications/nistpubs/800-82/SP800-82-final. pdf

Weiss, J. (2010). *Protecting industrial control systems from electronic threats (1 st Ed.)* . New York: Momentum Press.