Information security and the national infrastructure

Politics

Case Study 2: Information Security and the National Infrastructure

The United States energy infrastructure strengths the international financial system of the twenty first century. In fact, in the absence of a secure energy supply, welfare and health sectors are under danger and the United States financial system is not able to work properly. Additionally, more than 80% of the nation’s energy infrastructure is possessed by the nation’s private sector (IDAHO, 2010).

In the past few years, the security issues and vulnerabilities regarding digital systems and networks have increased exponentially, as the public responsiveness has not kept up by those innovative dangers and vulnerabilities in the Internet based cyberspace. However, these risks and dangers can influence all regions of public and private life, global and national companies and even security strategies of national states or international businesses similar to the OSCE. In the very old resist among defender and attacker, the attacker above ever comes into view to have the benefits by being well armed, generously deciding the strength of the attack and the target and without constraints of geographical distances and frontiers (European Academy, 2012; Eckert, 2010).

In addition, the Federal Government administrator has approved actions against security and vulnerability based issues which have become more and more critical for national infrastructure in the United States began by the PDD (Presidential Decision Directive/NSC-63) on CIP (Critical Infrastructure Protection), approved by Bill Clinton in 1988. Additionally, the managerial synopses of those directives involve the protection of national natural resources for better corporate management and handling (Dixon, 2010;

European Commission, 2012; Tabansky, 2011).

Moreover, national critical infrastructures are based on cyber or physical systems that are essential to the lowest processes of the financial and government departments. In this scenario, these departments comprise, however are not limited to, energy, telecommunications, finance, banking, water, transportation and emergency systems and services; in cooperation with private and government. Additionally, the majority of nation’s important infrastructures have traditionally been logically and physically detached systems that had small mutual dependence. However, in result of advancements in information technology and the need of increased performance, these arrangements have turned out to be more and more interlinked and automated. On the other hand, these innovations and developments have also created a wide variety of vulnerabilities in the forms of technology based system failure, weather, human error and other natural reasons, and cyber and physical security based attacks. Hence, tackling these issues and vulnerabilities will essentially need flexible, evolutionary methods that consider both the private and public sectors, and secure both global and domestic security (Dixon, 2010; European Commission, 2012; Tabansky, 2011).

Furthermore, processing and acquisition jobs are two important aspects of Supervisory Control and Data Acquisition System (SCADA). Through this system, control centers are capable of recognizing and repairing technology based interferences, in an attempt to develop the essential measures of technology based systems repair centrally and to have data relevant for planning and further accomplishments. Historically, every power plant had

its own technology management security control center linked with others' decisions of corporate networks. Hence, such initiatives can ensure the effective security and privacy management of the corporation (Umbach, 2010; Dallaway, 2009).

References

Dallaway, E. (2009, June 29). Using Information Security to Protect Critical National Infrastructure: Energy Sector is Hackers' Biggest Target. Retrieved October 22, 2012, from http://www. infosecurity-magazine. com/view/2310/using-information-security-to-protect-critical-national-infrastructure-energy-sector-is-hackers-biggest-target-/

Dixon, M. (2010, July 13). Information Security in the Oil and Gas Critical Infrastructure Protection (CIP) Sectors. Retrieved October 24, 2012, from http://www. discoveringidentity. com/2010/07/13/information-security-in-the-oil-and-gas-critical-infrastructure-protection-cip-sectors/

Eckert, S. (2010). Protecting Critical Infrastructure: The Role of the Private Sector. Retrieved October 24, 2012, from http://www. ridgway. pitt. edu/LinkClick. aspx? fileticket= Bezaq7AdjxA%3D&tabid= 233

European Academy. (2012, September 28). Brochure National Critical Energy Infrastructure Protection in Europe. Retrieved October 23, 2012, from http://www. euroakad. eu/fileadmin/user_upload/dateien/seminars/National_Critical_Energy_Infrastructure_Protection_in_Europe_DM. pdf

European Commission. (2012). Energy infrastructure. Retrieved October 22, 2012, from http://ec. europa. eu/energy/infrastructure/critical_en. htm

IDAHO. (2010). National Infrastructure Protection Plan Energy Sector.

Retrieved October 22, 2012, from http://www. bhs. idaho. gov/Pages/Plans/CIKR/Energy. pdf

Tabansky, L. (2011). Critical Infrastructure Protection against Cyber Threats. Retrieved October 22, 2012, from http://www. inss. org. il/upload/(FILE)1326273687. pdf

Umbach, F. (2010). Critical Energy Infrastructure Protection in the Electricity and Gas Industries – Coping with Cyber Threats to Energy Control Centers. Retrieved October 23, 2012, from hawk. ethz. ch/.../Critical_Energy_Infrastr_Umbach_Au10. pdf