Case and Trends Study for Establishing Cyber Security Information Sharing System

Soo Min Lim* and Chae Chang Lee

Korea Institute of Nuclear Non-proliferation and Control, 1534 Yuseong-daero, Yuseong-gu, Daejeon, Republic of Korea

*s2min@kinac.re.kr, chiching@kinac.re.kr

1. Introduction

Cyber threats that occur worldwide are becoming more diverse in their threat forms and attack targets. In recent years, the demand and necessity of research for timely response has been increasing due to the increase of cyber attacks targeting the infrastructure in overseas. However, it is not easy to take various evolving attacks and to formulate countermeasures against which infrastructure are quite differentiated from the general IT infrastructure. For this reason, the importance of sharing information related to past incidents including cyber incidents and recovery processes is emerging. The purpose of this paper is to review the requirements of the European institutions and the United States that have established an information sharing system preemptively and to utilize them to build cyber threat information sharing system in domestic nuclear facilities.

2. Precedent Case and Trends Study for Information Sharing System

2.1 General information

In nuclear facilities, timely response to safety is important. In particular, Korea's nuclear facilities have been strengthened in response to the cyber incident in 2014, when KHNP data were leaked as an example of cyber security infringement. In order to cope with an effective cyber-infringement incident, a corresponding system should be established through a series of processes, such as preparation-detection-initial response-recovery. This series of process requires knowledge of threat attributes and actual attack cases, but due to the nature of the nuclear industry, it is difficult to collect such information easily. Therefore, this paper overlook at the status of sharing information gathered by other international organizations including cyber events and IAEA member countries in the world, and establish information sharing system of domestic nuclear facilities and other infrastructure.

2.2 IAEA

The IAEA is developing a draft recommendation to establish cyber incident information sharing system related to nuclear security for cyber incident information sharing. The detailed information of the sharing information system would refer from the IAEA Computer Security Plan (2016-2018) [1], Computer Security Implementation Plan (2016-2018) for cyber security implementation plans.

2.3 EU Research Activities for Information Sharing System

According to the ENISA annual report 2016 [2], information sharing research for cyber security incidents are progressed in various EU nations, such as Netherlands (NCSC, National Cyber Security Centrum) [3], Germany (UP KRITIS) [4], Finland (FICORA, Finnish Communications Regulatory Authority) [5], Belgium (CTRISRP, Cyber Threat Intelligence Research Project) [6], and the Czech Republic (CZ NSA) [7].

2.3.1 UP KRITIS (Germany). Various countries around world, such as Canada, Australia, South Africa, Finland, France, Japan, India and the Netherlands has established a national security strategy through cyber security private-public partnership (PPP). As part of the European SCADA and Control System Information Sharing (E-SCSIE), Germany adopted a more specific approach to the partnership mechanism and submitted a recommendation to the National Cyber Security Council with a clear charter. UP KRITIS is developing a strategic cyber security solution by a specialist in order to avoid overlooking new security threats with a mature civil-public partnership space.

2.3.2 EU DENSEK Project (EU ISAC). The Information Sharing Platform will form a trusted network to liaise between the ISAC and its members. It will facilitate the distribution of information, newsletters, alerts etc. It provides the members of the Energy ISAC possibilities to stay informed regarding cyber security news and events in an efficient and effective way[8].

2.4 US NIST SP800-150

NIST SP 800-150 [9], "Guide to Cyber Threat Information Sharing", encourages greater sharing of cyber threat information among organizations, both in acquiring threat information from other organizations and in providing internally-generated threat information to other organizations. Recommendations described in this paper enables organizations to make more efficient and effective use of information sharing capabilities.

3. Experience and Plan for Computer Security Incident Response in ROK

Legal basis of incident response in ROK are following Act on Physical Protection and Radiological Emergency (APPRE).

3.1 Incident Experience

By a group calling itself “Who am I” who seems rebel to the nuclear power plant operation, releasing KHNP information to public in 2014. The incidents breaks irregularly 10 times more until the august of 2015. The cooperative government investigation team stating that ongoing leaks of NPP information were the work of a North Korean hacker’s organization.

3.2 KINAC/RS-015

As part of operational security measures in 2.5.6 of KINAC/RS015 [10], nuclear power operators should work with cyber security related organizations to share information on the latest cyber security threats, vulnerabilities, accidents, technologies, techniques, and countermeasures.

4. Conclusion

According to Cisco's white paper on how to respond to security threats to public utilities and energy industries, infrastructure that has undergone a security breach is likely to apply security measures, including application whitelisting, security solutions, and process safety reviews[11].

In general, the facility are opposed to considering an information sharing. Especially, for sharing cyber security issues between different institutes are sensitive information that the vulnerability of facility may expose classified information to the public and the information abasement.

For this purpose, it is recommended to establish a trusted channel and interagency body and to share information among different institutions.

REFERENCES

[1] Computer Security at Nuclear facilities, IAEA Nuclear Security Series No. 17.

[2] "ENISA Annual Report 2016", September 09, 2016.

[3] NCSC, https://www.ncsc.nl/english (last access date: 31 March 2017).

[4] http://www.kritis.bund.de/SubSites/Kritis/EN/publications/Fortschreibungsdokument_engl..html (last access date: 31 March 2017).

[5] https://www.viestintavirasto.fi/en/cybersecurity/ficorasinformationsecurityservices/cert-fi/rfc2350.html (last access date: 31 March 2017).

[6] http://www.politiestudies.be/userfiles/20141202%20BISC%20Luc%20Beirens%20voor%20verspreiding.pdf (last access date: 31 March 2017).

[7] http://www.nbu.cz/en/ (last access date: 31 March 2017).

[8] "Security Information Sharing for Smart Grids developing the Right Data Model", the 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014), 2014.

[9] "Guide to Cyber Threat Information Sharing", NIST Special Publication 800-150, October 2016.

[10] Regulatory Standard for Security for Computer and Information System of Nuclear Facility, KINAC/RS015, October 2014.

[11] Utility and Energy Security: Responding to Evolving Threats, 2016.