Preparation for Cyber Security Incident Response Training in Nuclear Power Plants

Jae-Gu Song*, Jung-Woon Lee , Cheol-Kwon Lee , Dong-Young Lee, Jong-Gyun Choi
Korea Atomic Energy Research Institute, Yuseong-gu, Daejeon 305-353, Republic of Korea
**Corresponding author: jgsong@kaeri.re.kr*

1. Introduction

As a part of International Atomic Energy Agency(IAEA) Coordinated Research Projects(CRP) [1, 2, 3, 4, 5], we have provided technical support to the IAEA International Training Course(ITC) on protecting computer based systems in nuclear security regimes by building incident response training programs and hands-on equipment. The IAEA ITC was developed for cyber security training in nuclear facilities. ITC is planned to be held every 18 months alternatingly at Idaho National Laboratory(INL) in the United States and at Korea Institute of Nuclear Nonproliferation And Control(KINAC) in the Republic of Korea.

This paper describes what to prepare for cyber security incident response training in nuclear power plants, based on our experience during the preparation of the programs and equipment for and the execution of the ITC that was held in the Republic of Korea in November 2019[6].

2. Preparation for Incident Response Training

2.1 Regulatory guide requirements for incident response training

The guides and standards (KINAC RS-015 and US NRC RG 5.71, IAEA, NEI, etc.)[7, 8, 9, 10] provide details on what to do for cyber security incident response training as part of operational and management security controls. The guides suggest that policies and procedures, plans, training, testing and drills, incident handling, monitoring, reporting, and incident response assistance should be addressed for the incident response in nuclear facilities.

The followings are the regulatory standard content for incident response training in KINAC RS-015. The Korean regulatory guide KINAC RS-015 requires the followings for incident response training.

A. Provide periodical education for the cyber attack incident response personnel

B. Based on the developed incident response procedure and virtual scenario, carry out periodical simulated drill (at least once a year) within the boundary with no influence on the nuclear facilities operation (including unnoticed drill)

C. Document education & training result

The regulatory guide also covers awareness training in separate sections. Descriptions of specialized cyber security training in the awareness and training section gives more detail information for incident response training, as follows;

A. Up-to-date skills and knowledge on data security, operating system security, application system security, network security, security controls, intrusion analysis, incident management and response, digital forensic, penetration testing, system functionality, etc.

B. Issues on the use of technology and tool for vulnerability mitigation, hardening cyber security for critical digital asset, and minimization of the consequences of the cyber attack

C. Technology to provide cyber security guide, guideline, and training to other employees

D. Technology to review cyber security controls and implementation

E. Technology to evaluate whether the critical digital asset complies with the cyber security controls

F. Technology for security controls design, acquisition, installation, operation, maintenance, and administration

2.2 Basic Requirements for incident response training

Based on the IAEA ITC preparation experience, the following activities are required to build an effective cyber security incident response training;

- Design target systems for incident response training with no influence on the nuclear facilities operation (Defining critical digital assets)
- Build target systems (with hypothetical power plants, virtual systems, mock-up systems, etc.)
- Develope attack scenarios (based on a realistic scenario that can occur)
- Develope attack code and program based on the attack scenarios (hands-on type exercises help to understand how to affected assets)
- Develope training documents (General documents for hypothetical power plants, target system design documents, templates for reporting, etc.)
- Build training feedback systems
- Make Training schedule
- Assign instructors

2.3 Detailed preparation items for IAEA ITC

According to the basic requirements for incident response training, the items have been prepared for the IAEA ITC as follows;

- Design of the condenser and condensate system for incident response training. Condenser receives the steam exhausted from the low-pressure turbine and cools it using the unit's cooling system. The condenser is also used to remove live steam in the case of certain transients such as a house load operation (loss of off-site power) or following a turbine trip.
- Development of a HIL system for cyber security incident response training in nuclear power plants according to designed condenser and condensate system. It includes hypothetical nuclear power plant simulations and specific system status simulations together with physical devices.
- Description of detailed exercise scenarios. It includes injection ID, timestamp, injection name and description, indicators of compromise, scenario implementation requirement. The exercise scenario considers the network zone and it was developed to affect the control of the power plant by compromised PLC in the HIL system.
- Penetration testing to the HIL system for finding vulnerabilities and development of exploits code based on the attack scenarios. The impact of the target system should be defined in detail, and the methods of attack trace considered for incident response training.

  - Development of training materials. The main documents are as follows;
    - Computer security incident response in NPP(Asherah),
    - Condenser and condensate system description,
    - Asherah high-level network architecture,
    - Consequence analysis for a critical digital asset – The Condenser System,
    - Detailed architecture diagram of the systems used in the exercise,
    - List of Sensitive Digital Assets(SDAs) on the condensers and their description,
    - Summary of the purpose of the condenser system and control behavior,
    - Guidelines for contacting the Asherah competent authority,
    - Outline incident response plan for Asherah,
    - Template for analysis results,
    - Template for describing threat scenarios,
    - Template for mitigation / corrective actions,
    - Template for post-incident analysis, etc.

  - Development of an attendance response/voting system for interactive training and address identified training gaps. All feedback information is managed on the training main server and it should be taken to help improve training.
  - *A detailed timetable.* It includes start time, duration, end time, location, description, requirements, whose actions, number of instructors.
  - Assignment of Instructors considering their expertise and experience. Normally, a lot of instructors are needed for hands-on type training. (At ITC, 25 instructors trained 32 participants)

3. Conclusions

Incident response training is important in nuclear facilities. In this paper, requirements and considerations for developing and conducting an effective incident training course are described based on the experience of IAEA ITC.

Acknowledgments

This work was supported by a grant from the Korea Ministry of Science and ICT, under the establishment and operation of cyber security attack response system at national nuclear facilities. (Project Number: 524480-20).

REFERENCES

[1] International Atomic Energy Agency, Enhancing computer security incident analysis at nuclear facilities, https://www.iaea.org/projects/crp/j02008 (accessed March 18, 2020).
[2] J. G. Song, J. W. Lee, C. K. Lee, J. G. Choi, A Data Classification and Analysis System for the Identification of Cyber Security Events in a Condenser and Condensate HIL System, International Atomic International Conference on Nuclear Security 2020, Feb. 10-14, 2020.
[3] Mitchell Hewes, Paul Smith, R. A. Busquim E Silva, Jianghai Li, J. G. Song, Beyond the Tank Level: Simulator and Hardware-in-the-Loop Supported Training for Computer Security of Nuclear I&C, International Atomic International Conference on Nuclear Security 2020, Feb. 10-14, 2020.
[4] R. A. Busquim E Silva, K. Shirvan, J. R. C. Piqueira, R. P. Marques, Development of the Asherah Nuclear Power Plant Simulator for Cyber Security Assessment, International Atomic International Conference on Nuclear Security 2020, Feb. 10-14, 2020.
[5] T. Holczer, G. Berman, S. M. Darricades, P. Gyorgy, G. Ladi, Virtualization-assisted testing of network security systems for NPPs, International Atomic International Conference on Nuclear Security 2020, Feb. 10-14, 2020.
[6] International Atomic Energy Agency, International Training Course for Protecting Computer Based Systems in Nuclear Security, https://www.iaea.org/events/evt1703440 (accessed March 18, 2020).

[7] KINAC/RS-015, Technical standard for the security of computer and information systems in nuclear facilities, Rev. 1, KINAC, 2014.
[8] Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, 2010.
[9] NEI 08-09 rev.6, Cyber Security Plan for Nuclear Power Reactors, Nuclear Energy Institute, 2010.
[10] International Atomic Energy Agency, Computer Security Incident Response Planning at Nuclear Facilities, IAEA, Vienna, 2016.