Current Status of the Cyber Threat Assessment for Nuclear Facilities

Hyundoo Kim*
Korea Institute of Nuclear Nonproliferation and Control (KINAC), 1534 Yuseong-daero, Yuseong-gu, Daejeon, Korea
**Corresponding author: hdkim@kinac.re.kr*

1. Introduction

In January 2014, one of the eight computers at Japanese Monju Nuclear Power plant control room was found to have malware infection. The infected system which stored electronic documents including employee's data sheets, over 42,000 emails and training logs was accessed over 30 times for five day.

In December 2014, unknown hackers hacked internal documents sourced from Korea Hydro and Nuclear Power (KHNP) and those electronic documents were posted five times on a Social Network Service (SNS). The data included personal profiles, flow charts, manuals and blueprints for installing pipes in the nuclear power plant. Although the data were not critical to operation or sabotage of the plant, it threatened people and caused social unrest in Korea and neighboring countries.

In December 2015, cyber attack on power grid caused a blackout for hundreds of thousands of people in Ukraine. The power outage was caused by a sophisticated attack using destructive malware called "BlackEnergy".

Cyber attacks are reality in today's world and critical infrastructures are increasingly targeted. Critical infrastructures, such as the nuclear power plant, need to be proactive and protect the nuclear materials, assets and facilities from potential cyber attacks.

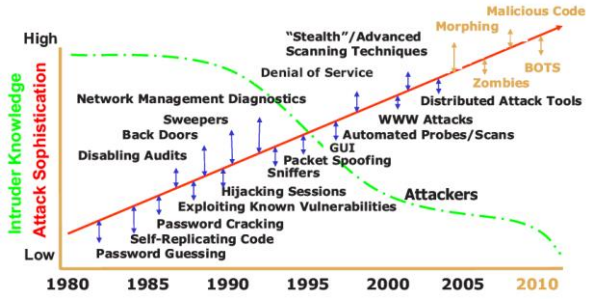

Fig. 1. Recent trend of cyber attacks

2. Background of Cyber Threat in Nuclear Power Plant

IAEA published international nuclear security recommendation, INFCIRC/225/Rev.4 which is intended to provide guidance to Member States (specially, competent authorities) on how to develop or enhance, implement and maintain a physical protection regime for nuclear material and nuclear facilities. It also recommends the development of a national Design Basis Threat (DBT) to design and evaluate physical protection system.

In addition, cyber attack is included as a new threat in revised INFCIRC/225/Rev.5 which is published in January 2011.

3. Recent Trend of Threat Assessment

The threat assessment is a formal process of gathering, organizing and assessing information about existing or potential threats that could result in or lead to a malicious act. Evaluation of the credibility of the information used in performing the threat assessment is critical. The output of threat assessment is a threat assessment document describing the overall threat environment and all known credible threats that need to be taken into consideration by the State. And then the DBT is developed or decided based on national threat assessment about potential adversaries and their motivation, intentions and capabilities.

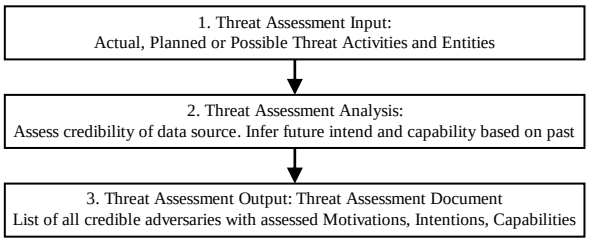

Fig. 2. The three steps for the threat assessment document

3.1. USA

The Nuclear Regulatory Commission (NRC) monitors intelligence information to keep abreast of foreign and domestic events and remains aware of the capabilities of potential adversaries to protect nuclear materials and facilities.

3.1.1. Annual Threat Environment Review

The NRC routinely reviews and analyzes a range of intelligence information. Particularly the Intelligence Liaison and Threat Assessment Branch annually prepares its assessment document for the threat environment and security events and formally provides its conclusions to the NRC called, "Annual Threat Environment Review".

3.1.2. Intelligence Community Liaison

The NRC also maintains routine contact with the Federal Bureau of Investigation (FBI), Department of Energy (DOE), Department of Homeland Security (DHS), Central Intelligence Agency (CIA), U.S. Customs Service, Defense Intelligence Agency, Department of Defense and other agencies concerned with terrorism, information sharing and planning.

3.2. Finland

The National Police Board in Finland is responsible for the maintenance of the threat assessment concerning malicious acts on and covering the use of unclear energy and use of radiation to be prepared for the DBT. The threat assessment is a description of the threat environment and the characteristics of persons and groups potentially engaging malicious acts. In addition, other assessments drawn by other authorities are used and known events of malicious acts and similar events which have targeted the use of nuclear energy and use of radiation are considered.

The Radiation and Nuclear Safety Authority (STUK) in Finland is responsible for the preparation and maintenance of the DBT.

3.3. UK

The Joint Terrorism Analysis Centre (JTAC) analyses and assesses all intelligence relating to international terrorism in domestic and overseas. The JTAC brings together counter-terrorist expertise from the police and government departments so information is analyzed and processed. The JTAC also maintains the civil nuclear security program and contributes to a regular production of a comprehensive nuclear threat assessment.

The Office for Nuclear Regulation (ONR) prepares UK's DBT – The Nuclear Industries Malicious Capabilities Planning Assumptions (NIMCA) based on the nuclear threat assessment by the JTAC.

3.4. Japan

The DBT working group is consist of National Police Agency (NPA) and Japan Coast Guard (JCG) as well as Nuclear Regulation Authority (NRA). The working group assesses the threat environment around and within Japan and reviews threat assessment and DBT annually.

3.5. Hungary

The Hungarian Atomic Energy Authority (HAEA) regularly assesses and determines and when necessary revises the threats of nuclear energy within Hungary based on the coordination with the Hungarian National Police, Military Security Office, Constitution Protection Office, Counterterrorist Centre and Nation Security Authority.

The HAEA reviewed the national threat assessment including cyber threats and issued the updated facility specified DBT by June 2015.

3.6. Korea

The Nuclear Safety and Security Commission (NSSC) conducts threat assessment and revises DBT considering the factors, probabilities and consequences of threat in every three years or when necessary.

The NSSC deputes to these works to the KINAC. The KINAC considered cyber threats as a new threats in threat assessment and DBT in 2012 and revised threat assessment and DBT in 2015.

The KINAC collects a large amount of cyber threat information through open source and cooperates with related domestic organizations for cyber threat information. Based on major cyber incident in the industry, collected information is categorized and evaluated for the credibility of cyber threat information. And the KINAC issues threat assessment document based on evaluated and screened information.

Threat assessment document consists of five chapters: introduction, trends and example of terror, analysis of domestic threats, other considerable factors and conclusions. The DBT is maintained or revised with working group by using threat assessment document.

4. Conclusions

The threat assessment document and its detailed procedure are confidential for the State. Nevertheless, it is easy to find cooperation on assessing and evaluating the threats of nuclear materials and facilities with other government departments or agencies including the national police.

The NSSC and KINAC also cooperated with the National Intelligence Service (NIS) and National Security Research Institute (NSR). However, robust cyber threat assessment system and regular consultative group should be established with domestic and overseas organization including NIS, NSR, the National Police Agency and the military force to protect and ensure to safety of people, public and environment from rapidly changing and upgrading cyber threats. The consultative group should regularly share the information about existing or potential cyber threats and maintain cyber threat.

REFERENCES

[1] Jeffrey Hahn, Donna Post Guillen, Thomas Anderson, "Process Control Systems in the Chemical Industry: Safety vs. Security", INL, 2005.
[2] IAEA Nuclear Security Series No. 13, "Nuclear Security Recommendations of Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev.5)", IAEA, 2011.
[3] IAEA Nuclear Security Series No. 10, "Development, Use and Maintenance of the Design Basis Threat", IAEA, 2009.
[4] U.S.NRC web site: http://www.nrc.gov/
[5] "The Design Basis Threat (DBT) and Threat Assessment", U.S.NRC, 2012.
[6] "Design basis threat for the use of nuclear energy and use of radiation", STUK, 2013.
[7] MI5 web site: http://www.mi5.gov.uk/
[8] "The state of security in the civil nuclear industry and the effectiveness of security regulation", ONR, 2011 – 2012.
[9] "Developing of Design Basis Threat and Current Physical Protection measures", NRA, 2012.
[10] "DBT development for a new nuclear power plant, including a cyber DBT", HAEA, 2015.