Contribution ID: **7** Type: **Paper**

FIRST NATIONAL EXERCISE IN COMPUTER SECURITY IN NUCLEAR SECTOR IN SLOVENIA

Whether we like it or not, acknowledge it or not, the number of cyber-attacks is increasing. Malicious actors are continuously becoming more sophisticated, highly motivated, some also well-funded, and focused on the nuclear sector. If cyber-attacks in the nuclear sector were to be successful, consequences of such an attack could potentially be catastrophic for people and the environment. Therefore, our efforts in computer security must increase. One example is conducting computer security exercises, which are an essential element in assuring a high level of computer security supporting nuclear security. The main objectives of exercises are awareness, testing internal procedures, identifying gaps in computer security measures, testing the efficiency of computer security plans and response arrangements, training the Computer Security Incident Response Team, etc. All of these objectives, and more, can be achieved by different types of exercises: table-top, drills, blue vs red, simulated and combined exercises, etc. To our knowledge, there were only a handful of computer security exercises conducted in the nuclear sector to date. In order to substantiate our beliefs, we conducted research, comprised of descriptive analysis of various publicly available sources, structured interviews with national and international experts in nuclear sector and verified our findings with emergency preparedness experts, employed at the Slovenian Nuclear Safety Administration. The results of our research represent a structured and comprehensive approach in preparation, conduct and evaluation of computer security exercises. Based on the results of the research, the first national exercise in computer security in nuclear sector in Slovenia called KIVA2019 was prepared. The exercise was conducted in January 2019 as a one-day table-top exercise with a short storyline and a cyber-attack scenario based on current computer security incidents in critical infrastructure. Exercise was attended by participants from all key national stakeholders in the nuclear sector: nuclear facility operators, competent authorities, technical support organizations and suppliers of computer software and hardware equipment. Due to the importance of this topic on a national level, the exercise was attended also by external observers from the Slovenian Ministry of Interior, Ministry of Public Administration and Faculty of Criminal Justice and Security. Evaluation of the exercise comprised of detailed analysis and an action plan, including further steps that are needed to fill in the gaps identified during the exercise. These gaps are not new to nuclear security and generally include the improvement of information sharing on a national and international level and harmonization of response arrangements for cyber-attacks by all key stakeholders in nuclear sector. Additionally, KIVA2019 represents a starting point for future computer security exercises in Slovenia. Knowledge gained from this research and KIVA2019 will contribute to the preparation of future exercises, enhance cooperation between key stakeholders, and thus improve computer security and nuclear security in the Slovenian nuclear sector and in general.

Gender

State

Slovenia

Authors: Mr TOMAŽIČ, Samo (Slovenian Nuclear Safety Administration); Dr BERNIK, Igor (Faculty of Criminal Justice and Security); Mrs TOMAŽIČ, Metka (Slovenian Nuclear Safety Administration)

Presenter: Mr TOMAŽIČ, Samo (Slovenian Nuclear Safety Administration)

Track Classification: CC: Good practices in the development and execution of nuclear security exercises (e.g. tabletop, drills and field exercises);