Contribution ID: **583** Type: **Interactive Content Presentation**

Cybersecurity in Research Centers: Focus on nuclear and radioactive facilities.

Cybersecurity in Research Centers: Focus on nuclear and radioactive facilities.

The Cybersecurity Research Center's standards for handling nuclear and radioactive materials should be built on a "defense in depth" model. This model should be suitable for the existing ecosystem and should consider all cyberthreats that can and undermine existing security, with the objective of compromising critical telecommunications infrastructure, information systems, nuclear control systems, and radioactive data research centers, eliminating and exposing sensitive data.

Cybersecurity in a nuclear and radioactive facility should focus on an in-depth defense model. Protective barriers or defenses should delay cyberattacks and complement the protection of critical infrastructures involving the control and management of nuclear and radioactive components, as well as the physics of administrative and security systems.
In order to develop in depth the defence model to protect the information and industrial control systems of nuclear and radioactive facilities, each of the layers of the proposed model must be analysed, giving the real value corresponding to each of the critical or vital assets, including each of the risks that may infringe the defined defence layers.

The defense model proposed in depth must be in a cycle of continuous improvement through planning, implementation, review and improvement actions. These actions aim to evaluate the original plan, add new critical infrastructures that have been identified, add new threats and registered security incidents.
The concept of in-depth defence applied to the field of nuclear safety comes from the latest "Three Mile Island" accident works. It is defined as a defence that includes three successive independent barriers that lead to an extremely low level of probability that an accident may have an off-site impact. The idea is that each safety device must be considered a priori as vulnerable and therefore must be protected by another device.
In order to establish a defence model in depth, the following definitions are proposed:
- The severity of a given value measures the real impact of the incident based on the criticality of the asset or the potential impact of the incident on the threatened fine.
- A measurement scale is proposed that establishes the levels of severity, with the objective of comparing the different security incidents generated by the impact. Users are responsible for determining the appropriate level of seriousness to be appreciated in light of the impact of the incident on the asset to be protected.
- A barrier is a security means capable of protecting a part of the information system against at least one threat. A barrier can be human, a method can be static or dynamic, and manual or automatic. It must have a means of control that shows the state of operation of the barrier.

- A line of defense is a set of barriers, and the overcoming causes an incident whose severity depends on the number of barriers still to be overcome by the threat or threats, in order to achieve a property or protected property.
- The defense in depth of information systems is a global and dynamic defense that coordinates several lines of defense to cover all the depth of the system.

State

Mexico

Gender

Male

Author: Mr PEREZ, Juan Manuel (National Institute for Nuclear Research)

Presenter: Mr PEREZ, Juan Manuel (National Institute for Nuclear Research)

Track Classification: CC: Information and computer security considerations for nuclear security