Contribution ID: **112** Type: **Paper**

The need for computer security at nuclear facilities

In light of the growing threat of attacks on the IT of critical infrastructures, states need to take steps into protecting systems that are vital to the safety and security of such installations. Nuclear facilities are just of one the installations, that are of particular interest to groups that are looking into either disabling a countries power grid or to actually try and cause physical damage and thereby possibly causing the release of radioactive material.
The capabilities of hackers are increasing with time, as tools developed and used by state actors are getting available, therefore the security of the IT infrastructure needs to be continuously monitored. For Nuclear facilities, a rigorous system is needed, in which the IT used in the facility is analyzed and hardened against attacks. Most nuclear power plants will have been built at a time, when threats through attacks on IT systems were unlikely or even impossible. In time, these installations were upgraded with IT systems, which now need to be analyzed as to the potential risk they might pose were an attacker to be able to gain access to or even control of such system. This can be a complicated and involved process that may take years.
In this presentation we will highlight the approach taken in Germany and point out the advantages that come with that approach.

State

Germany

Gender

Male

Primary authors: Dr MERGEL, Edgar (BMU); ELSNER, Thomas (BMU)

Presenters: ELSNER, Thomas (BMU); KROEGER, Helge

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