

Cyber Security Exercise Georgius 2019

Summary

Executing physical security exercises is common practise at nuclear facilities. Executing cyber security exercises is still less common. In 2019 Urenco Nederland B.V. organised cyber security exercise "Georgius 2019", a multidisciplinary security exercise. The exercise stretched over 3 days and was conducted over in the field. It involved several departments and processes of URENCO Netherlands, as also a range of emergency response and crisis management processes from the public domain. The presentation will explain why this exercises was organised, how it was executed and what the main points were that participants took form this exercise.

Scope of the exercise.

Urenco Nederland B.V. sees doing exercises as essential in ensuring that it's security measures and the organisation around that are fit for purpose. It gives both the opportunity to train Urenco staff in the right behaviour during unusual and sometimes difficult situations, as that it also demonstrates to Urenco's General Management and to other stakeholders like the nuclear security regulator that Urenco Nederland B.V.'s security performance is effective to counter the defined threat.

Recently, like in many countries, in the Netherlands there have been made substantial steps in updating cyber security regulation. And not only nuclear facilities themselves, but also emergency response units from the public domain are getting more and more aware that also their effectiveness partly rests on IT support those public emergency response processes need.

This is the core idea behind Georgius 2019, exercising the additional requirements that where made more explicit in recent updates of nuclear security regulation like for instance forensic in the cyber domain as also exercising the impact of a cyber threat (for instance a crypto locker) for emergency response units in the public domain.

Organising the exercise

Organising a multidisciplinary, 3 day long security exercise in the field is a challenge. The presentation will describe what approach was used to bring the different organisations participating in the exercise together and how consensus was reached on what the exercise should do and how it should be organised and conducted.

Executing the exercise

The presentation will also explain how the exercises was executed. So, how the exercise organisers ensured that actions at different locations remained synced in the overall exercises scenario. And it will explain how the evaluation was organised of the exercises which took place on multiple locations in the field.

Lessons learned

And of course the presentation will give an overview of the type of lessons that were learned and will give ideas to maximize the learning effect of other exercises in future.

State

Netherlands

Gender

Male

Primary author: KEIZER, Antonius (URENCO Nederland B.V.)

Presenter: KEIZER, Antonius (URENCO Nederland B.V.)

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