Authority for Nuclear Safety and Radiation Protection

Evaluation of threats in the nuclear domain of the Netherlands

Marco Schraver

Nuclear Security Policy Coordinator

Authority for Nuclear Safety and Radiation Protection (ANVS)

The Netherlands

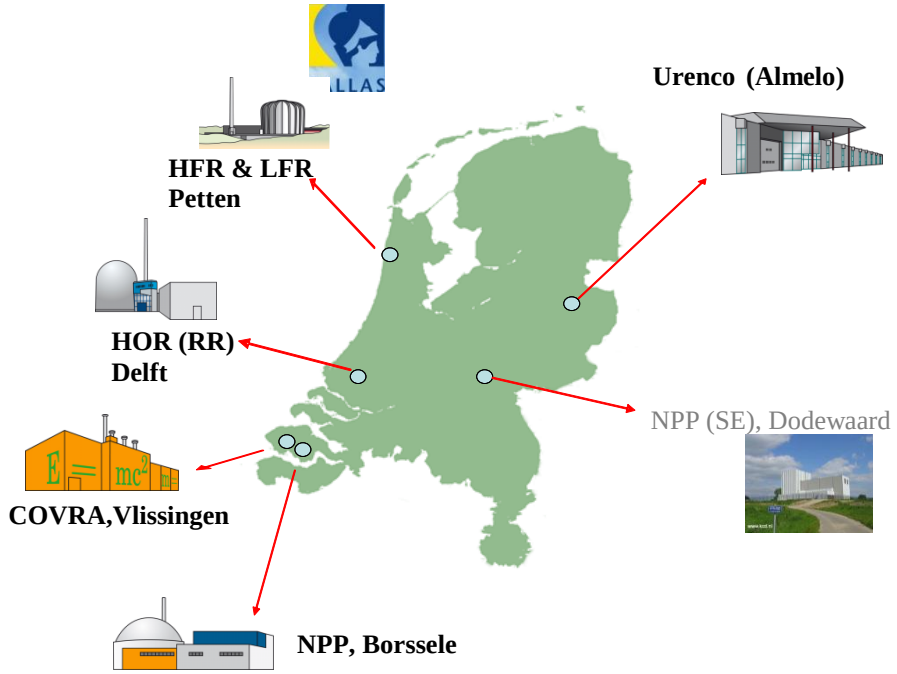
Unclassified Information

Content of the presentation

- Introduction of the nuclear domain in the Netherlands
- Public and Private Partners
- Legal framework
- The Crown Jewels
- DBT development of content
- Increase of the attack surface
- Points of attention

Intro: Nuclear Installations in the Netherlands

- NPP Borssele (2 loop PWR, 510 MW_e)
- NPP Dodewaard shutdown (BWR, safe enclosure)
- Research Reactor HFR Petten (50 MW_{th})
- Research Reactor LFR Petten (30 kW_{th}), shutdown
- University Reactor HOR Delft (3 MW_{th})
- Ultra Centrifuge Enrichment Plant URENCO (UNL)
- Interim Waste Storage Facility (COVRA)
- PALLAS Research Reactor (design phase)



Partners in the Netherlands nuclear domain

Public partners

- National Coordinator for Security and Counterterrorism (NCTV)
- National Cyber Security Centre (NCSC)
- General Intelligence and Security Service (AIVD)
- National Police (High Tech Crime Unit)

- Ministery of Foreign Affairs

Private partners

- License holders

Regulator

- Authority for Nuclear Safety and Radiation Protection (ANVS)

Legal framework

- CPPNM/a
    - Ratified in 2011
    - Final implementation in legislation in 2015

- Ministerial Regulation Security of Nuclear Installations and Fissile Material (legal)

  => Compliant with CPPNM/a

- Design Basis Threats (legal)
    - Physical Protection (2010, 2015, *2020*)
    - Cyber Security (2016, 2018, *2020*)

- Implementation Guide DBT Cyber Security (non-legal)

DBT process

What's a Design Basis Threat in the Dutch context?

A description of:

- the most serious, yet conceivable, threats;
- adverseries, their motives, goals, financial, technological and network capabilities;
- the vulnerable components of the nuclear installation;
- the most valuable elements of the nuclear installation (IT, OT);
- Etc.

- Primary adversaries in the DBT-approach: non-friendly states!

- Periodic evaluation and review of DBTs (Physical 5 years, Cyber 2 years)
- Interim adjustment DBT always possible

The Crown Jewels

Types of valuable/sensitive elements:

- primary processes / vital infrastructure (e.g. OT)

  => disruption of continuity/radiological emission

- sensitive/confidental information (e.g. IT)

  => prelude to attack / theft

- information on lay-out of the installation

  => national and on site security

- financial and economic information of the license holder

  => economic espionage

DBT development of content

- Design Basis Threats (legal)

  - Physical Protection (2010, 2015, *2020*)
    => Focus on primary adversaries groups
    => Goals, motives, capabilities etc.
    => Relatively few changes, with the exception of drones

  - Cyber Security (2016, 2018, *2020*)
    => Rapid developments in terms of the extent and depth of the cyber threat
    => Increasingly stronger interdependence between physical and cyber threat (stepping stone, blended attacks)
    => Increase of the attack surface

Increase of the attack surface

- The **attack surface** of a software environment is the sum of the different points (the "attack vectors") where an unauthorized user (the "attacker") can try to enter data to or extract data from an environment.
- *Keeping the attack surface as small as possible is a basic security measure.*
- Increase of the attack surface means:

  => Increase in points of entry in IT-, OT, Cloud services etc.

  => Transition from analogue systems to digital + outsourcing of services

  => Increase in number of attackers, level of professionalization, strength, knowledge, availability on Internet / Darknet Reduction of costs for carrying out an attack

  => limited increase in knowledge and awareness among government and licensee to keep up with the increase in threat/attack possibilities

  => Almost impossible to keep up with developments and innovations

  => Licensee staff -> limited knowledge -> hiring external

Points of attention

- Shift of focus from physical security to cyber is necessary.
- More attention is needed in the development of security with regard to Cloud, Stepping Stone, Blended Attacks, Suppliers etc.
- Exchange of information between public and private parties (threat analyzes, incident reports, etc.) is key for the further development of cyber security.
- More cyber awareness on a permanent basis is necessary within companies al all levels.
- Strengthening the integration of physical and cyber security within companies.

- I thank you for your attention!