De veiligheid en beveiliging van de Belgische kerncentrales: het FANC preciseert de recente berichtgeving

24 November 2016

Geplaatst op de website van het FANC (de Belgische toezichthouder voor nucleaire veiligheid). Het FANC geeft hierin toelichting op de recente berichtgeving in de media.

Het FANC bevordert de doeltreffende bescherming van de bevolking, werknemers en het leefmilieu tegen het gevaar van ioniserende straling. Het agentschap waakt dus over de nucleaire veiligheid en beveiliging en ziet er op toe dat de exploitanten van nucleaire installaties hun wettelijke verplichtingen op vlak van zowel de veiligheid als de beveiliging nakomen. Het is in dit kader dat er de afgelopen weken meerdere berichten in de media zijn verschenen. Daarbij werden verschillende dossiers en technische termen aangehaald die om verduidelijking en toelichting vragen.

1. Veiligheid en beveiliging

Nucleaire veiligheid en beveiliging zijn niet hetzelfde. Nucleaire veiligheid omvat alle maatregelen die genomen worden bij elk aspect van de nucleaire installaties, om zo incidenten en ongevallen te voorkomen en, indien toch, de gevolgen daarvan maximaal te beperken. Veiligheid beoogt dus de bescherming van de bevolking, werknemers en het leefmilieu tegen het gevaar van ioniserende straling en omvat zo ook technische maatregelen voor het optimaliseren van het afvalbeheer. Nucleaire beveiliging bevat dan alle maatregelen om inbraak, diefstal, sabotage en andere kwaadwillige handelingen te voorkomen, tijdig te detecteren en erop te reageren.

2. Erkenningen

Volgens het **KB van 17 oktober 2011 betreffende de fysieke beveiliging van het kernmateriaal en de nucleaire installaties** dienen de exploitanten van nucleaire installaties en transportbedrijven bij het FANC een aanvraagdossier in voor de erkenning van hun systeem voor de fysieke beveiliging. Exploitanten hebben tot uiterlijk 1 mei 2017 de tijd om maatregelen te treffen en verbeteringen uit te voeren in het kader van deze erkenningsprocedure. In tussentijd evalueert het FANC het ingericht fysiek beveiligingssysteem en doet het een uitspraak over de erkenningsaanvraag.

Op basis van de meest recente evaluaties van het fysiek beveiligingssysteem van Electrabel besliste het FANC op 1 november 2016 om voorlopig geen erkenning toe te kennen. Dit betekent niet dat het niveau van het huidige beveiligingssysteem niet behoorlijk is, maar het FANC ziet nog ruimte voor verbetering. Electrabel heeft nu drie maanden de tijd om de aanpassingen die het agentschap heeft aanbevolen door te voeren aan het fysiek beveiligingssysteem. Het FANC volgt dit analyseproces van nabij op en zit hierover geregeld samen met Electrabel.

Het doel van deze erkenningsprocedure is tweeledig. In de eerste plaats moet de reeds strenge beveiliging van nucleaire installaties en transporten beantwoorden aan een nog hoger niveau. Daarnaast is het belangrijk dat alle werknemers zich houden aan een optimale beveiligingscultuur. De implementatie van deze beveiligingscultuur werd door Electrabel opgenomen in speciaal daarvoor ontwikkelde programma's.

3. Veiligheidsattesten en veiligheidsmachtigingen

Electrabel beschikt dus nog niet over een erkenning van haar fysiek beveiligingssysteem, maar is wel in het bezit van een veiligheidsmachtiging.

Een veiligheidsmachtiging wordt toegekend aan personen en organisaties die om beroepsredenen toegang moeten krijgen tot de veiligheidszones van een nucleaire inrichting, tot kernmateriaal of tot vertrouwelijke documenten. Het onderzoek voor het verkrijgen van een veiligheidsmachtiging gebeurt door de **Nationale Veiligheidsoverheid** (NVO). Aangezien dit onderzoek meerdere maanden in beslag kan nemen, levert het FANC tijdige veiligheidsattesten en toegangsvergunningen af om deze wachtperiode te overbruggen.

4. Documentenbeheer

Het FANC voerde recent een inspectie uit bij de hoofdzetel van ENGIE Electrabel in Brussel om het systeem voor documentenbeheer te controleren. Het agentschap stelde vast dat ENGIE Electrabel beschikt over een efficiënt en goed gedocumenteerd systeem voor het beheer van nucleaire documenten, maar dat er nog ruimte voor verbetering is.

5. Cyberbeveiliging

Cyberbeveiliging is een specifiek luik binnen de nucleaire beveiliging. Het wordt niet letterlijk vermeld in de wetteksten. In het **KB van 17 oktober 2011 houdende de categorisering en de bescherming van nucleaire documenten** staat dat de installatie/transporteur de nucleaire documenten moet beschermen, dus ook de digitale documenten. Daarnaast werd cyberbeveiliging opgenomen in de stresstests van 2011; op basis daarvan namen de nucleaire exploitanten reeds maatregelen.

Zoals besproken in de subcommissie 'Nucleaire Veiligheid' zijn de besturingssystemen in het nucleaire gedeelte van de kerncentrales zijn analoog en niet aangesloten op een externe server. Ze zijn totaal geïsoleerd en kunnen dus nooit het onderwerp uitmaken van een cyberaanval. Andere systemen, zoals bijvoorbeeld het mailsysteem, zijn wel verbonden met de buitenwereld en daarom wordt de nodige aandacht besteed aan cyberbeveiliging. Aangezien dit in constante evolutie is, moeten de dreiging en de getroffen maatregelen op regelmatige basis geëvalueerd en aangepast worden in functie van de meest recente indicaties. Binnen het FANC en zijn technisch filiaal Bel V zijn verschillende cyberexperts aan de slag. Het agentschap plant verdere acties om cyberbeveiliging nog strenger aan te pakken. Het FANC werkt hiervoor samen met het Centrum voor Cybersecurity België (CCB) en wisselt hierover ervaringen uit met de buitenlandse collega-autoriteiten.

Het is bovendien belangrijk om een onderscheid te maken tussen cyberbeveiliging en cybercriminaliteit. Het FANC werkt vanuit haar missie en wettelijke opdracht aan de cyberbeveiliging. Het beveiligen houdt enerzijds in dat de digitale systemen worden beschermd tegen inbraak, diefstal en beschadiging van de hardware, software en informatie op deze systemen, als het verzekeren van de beschikbaarheid van de digitale systemen en de informatie erop anderzijds. Cybercriminaliteit daarentegen is dan (een poging tot) het plegen van een misdaad aan de hand van een computer en een netwerk. Cybercriminaliteit behoort niet tot de wettelijke bevoegdheid van het FANC, maar het FANC werkt wel nauw samen met andere overheden (bijv. politie) om (pogingen tot) criminaliteit vast te stellen.

6. Brieven ter attentie van Electrabel

De media berichtten ook over twee brieven van het FANC aan Electrabel. In beide brieven drukte het FANC zijn bezorgdheid uit over de veiligheid in de Belgische kerncentrales en over de houding van Electrabel ten opzichte van de veiligheidscultuur. In het kader van de veiligheidscultuur stelde het FANC afgelopen jaar twee pro Justitia's op tegen Electrabel, omdat de veiligheidsprocedures niet rigoureus werden toegepast in de kerncentrale van Tihange. Het agentschap wil echter benadrukken dat er nooit een reëel gevaar is geweest, maar het FANC hanteert de strengste normen qua nucleaire veiligheid. De brieven dateren van afgelopen zomer. en intussen heeftHoewel het FANC intussen heeft vastgesteld dat Electrabel reeds acties ondernam om tegemoet te komen aan de opmerkingen uit deze twee brieven, moeten er nog steeds cruciale stappen worden genomen. Het FANC volgt dit verder van nabij op.

7. Besluit

Het FANC hanteert het basisprincipe dat de exploitant de primaire verantwoordelijke is voor de nucleaire veiligheid en beveiliging. De fysieke beveiliging van nucleaire installaties, transporten en documenten voldoet aan de normen om te beantwoorden aan de huidige dreiging. De maatregelen in het kader van de nucleaire beveiliging worden opgebouwd, zo treffen de nucleaire exploitanten nu bijkomende maatregelen die in de toekomst standaard moeten worden. De aanpak van de nucleaire veiligheid en beveiliging is nooit afgerond. Dit is een continu proces, het continu aanpassen van de standaarden, een systeem van continue verbetering.