Autoriteit Nucleaire Veiligheid en
Stralingsbescherming

Handreiking BRAS

Beveiliging Radioactieve Stoffen (BRAS)

Voorwoord

In 2018 vond een wijziging van regelgeving plaats. Daardoor was de bestaande ‘Handreiking beveiliging radioactieve stoffen’ van 22-07-2013 niet meer actueel. Daarnaast had ook het werkveld behoefte aan een aanpassing van de handreiking. Om de handreiking zo goed mogelijk aan te laten sluiten op de behoefte van toekomstige gebruikers, is deze gereviseerde versie in concept aan hen voorgelegd.

Met deze handreiking wordt primair de beveiligingsverantwoordelijke op weg geholpen om te voldoen aan de wettelijke voorschriften met betrekking tot het beveiligen van radioactieve stoffen.

April 2021
Bernd Keller, afdelingshoofd Stralingstoepassingen

Inhoud

1 Inleiding

Handreikingen zijn informatieve documenten, die de ANVS ten behoeve van vergunninghouders publiceert en waarin staat beschreven hoe de ANVS tegen een bepaald onderwerp aankijkt. De vergunninghouder kan de handreiking vervolgens als uitgangspunt nemen bij het opstellen van zijn documenten en bij zijn handelen. Handreikingen zijn niet aan een vergunning of de wet verbonden en hebben geen verplichtend karakter.

De handreiking BRAS (hierna: de handreiking) geeft onder meer toelichting op en uitleg over wettelijke bepalingen, het beveiligingsplan en bij wie welke verantwoordelijkheden liggen. Hiermee beoogt de ANVS duidelijkheid te geven over wat van u wordt verwacht om te voldoen aan de (doel)voorschriften van beveiligingsparagraaf 4.3.4 van de ANVS Verordening basisveiligheidsnormen stralingsbescherming (hierna: ANVS-verordening).

1.1. Veiligheid en beveiliging

De ANVS-verordening heeft tot doel de veiligheid te borgen van de vergunninghouder en zijn of haar omgeving bij het gebruik van radioactieve stoffen. Radioactieve stoffen kunnen immers bij foutieve fabricage, onjuist gebruik, verkeerde opslag of een slecht georganiseerd (intern) transport schade aan de gezondheid van mens en/of milieu veroorzaken.

Op zowel internationaal als nationaal niveau zijn veiligheidsadviezen en richtlijnen opgesteld voor het gebruik van radioactieve stoffen. Het accent ligt in deze adviezen en richtlijnen vaak op veiligheid, waarmee bescherming van mens en milieu tegen de schadelijke effecten van ioniserende straling bedoeld wordt. In deze handreiking hebben wij het over beveiliging tegen misbruik, sabotage of diefstal van radioactieve stoffen, afgekort door BRAS (beveiliging radioactieve stoffen).

1.2. Leeswijzer handreiking

In deze handreiking wordt op verschillende momenten verwezen naar literatuur. Een overzicht van deze literatuur is opgenomen in bijlage A.

Deze handreiking is als volgt opgebouwd:

1. Voor wie en bij welke toepassing is handreiking bedoeld? (hoofdstuk 2)
2. Wet- en regelgeving voor BRAS (hoofdstuk 3)
3. Wat staat er in die beveiligingsparagraaf 4.3.4 (hoofdstuk 4)
4. Het proces om tot een goede beveiliging te komen (hoofdstuk 5)
5. Hoe u de beveiliging concreet regelt volgens de wetgeving (hoofdstuk 6)

2 Voor wie en bij welke toepassing is deze handreiking bedoeld?

Deze handreiking is met name geschreven voor de aangewezen beveiligingsverantwoordelijken van de houders van een vergunning op basis van de Kernergiewet[1] (hierna: vergunninghouders).

Een beveiligingsverantwoordelijke is en blijft op de hoogte van de regelgeving en volgt nieuws en ontwikkelingen hierin. Een beveiligingsverantwoordelijke is bewust van de belangen van de organisatie en de bescherming van deze belangen en heeft voldoende kennis / technische expertise; niet per definitie om alles zelf uit te voeren, maar wel om de kwaliteit en naleving van de genomen maatregelen goed te kunnen beoordelen. Daarnaast is de samenwerking met de stralingsbeschermingsdeskundige, gelet op beider expertise, essentieel voor het kunnen opvolgen van deze handreiking.

2.1. Toepassing van de handreiking

Beveiligingsparagraaf 4.3.4 is uitsluitend van toepassing op handelingen met kunstmatige radioactieve categorie 1-, 2-, of 3-stoffen en is niet van toepassing op handelingen met natuurlijke bronnen, handelingen met toestellen en het vervoer[2] van radioactieve stoffen.

De radioactieve stoffen worden op basis van bijlage 4.1 van de Regeling basisveiligheidsnormen stralingsbescherming (Rbs) gecategoriseerd in drie beveiligingsklassen. Er is aangesloten bij de internationaal geaccepteerde systematiek van de IAEA [IAEA03]. De categorie-indeling wordt per ruimte bepaald (sommatie). Hierbij moet worden uitgegaan van wat er per opslag is vergund, niet van wat er daadwerkelijk aanwezig is.

Als de radioactieve stoffen niet op basis van bijlage 4.1 Rbs kunnen worden gecategoriseerd, dan is voor deze stoffen geen beveiligingsplan vereist en zijn er geen aanvullende beveiligingsmaatregelen nodig. De vergunninghouder is nog wel gehouden aan de algemene zorgplicht voor de beveiliging zoals beschreven in artikel 4.4, derde lid, van het Besluit basisveiligheidsnormen stralingsbescherming (Bbs).

Ondernemers kunnen ervoor kiezen de beveiliging van radioactieve stoffen in te richten op basis van de 'Verbeterde Risico-KlassenIndeling' (VRKI) van het Centrum voor Criminaliteitspreventie en Veiligheid (zie website CCV). In dat geval moet deze handreiking naast de meest recente VRKI-publicaties gelezen worden. Deze handreiking gaat verder niet in op de VRKI en dient ook niet ter vervanging van de VRKI.

[1] De inhoud van deze handreiking is niet van toepassing voor zover de Regeling beveiliging nucleaire inrichtingen en splijtstoffen van toepassing is.

[2] Buiten een locatie kunnen er (ook) beveiligingseisen gesteld worden aan vervoer. Deze vallen buiten het bereik van de handreiking

3 Wet- en regelgeving voor beveiliging radioactieve stoffen

3.1. Europa over Chemische Biologische, Radioactieve en Nucleaire stoffen

Op Europees niveau vinden al enige tijd initiatieven plaats ter versterking van de weerbaarheid tegen terroristische dreigingen met chemische, biologische, radiologische en nucleaire middelen (CBRN-stoffen/middelen). De Europese Ministers van Justitie en Binnenlandse Zaken hebben bijvoorbeeld ingestemd met een actieplan van de Europese Commissie over dit onderwerp. Dit actieplan wordt in Nederland door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en de verschillende betrokken ministeries geïmplementeerd. Het plan beschrijft een samenhangende aanpak op Europees niveau om de kans op een aanslag of ongeluk met CBRN-stoffen/middelen te verkleinen.

3.2. Nationale wet en regelgeving beveiliging radioactieve stoffen

Naast ontwikkelingen op internationaal niveau, hebben we in de Nederlandse wet- en regelgeving opgenomen hoe om te gaan met de beveiliging van radioactieve stoffen.

De hoofdlijnen op het gebied van beveiliging van radioactieve stoffen zijn in het Besluit basisveiligheidsnormen stralingsbescherming (Bbs) te vinden. Nadere uitwerking van voorschriften uit het Bbs is geregeld in drie ministeriële regelingen en een ANVS-verordening: de Regeling basisveiligheidsnormen stralingsbescherming (Rbs), de Regeling stralingsbescherming beroepsmatige blootstelling 2018, de Regeling stralingsbescherming medische blootstelling en de ANVS-Verordening basisveiligheidsnormen stralingsbescherming.

In de ANVS-verordening worden, op basis van de hoofdlijnen in het Bbs, nadere regels met betrekking tot organisatorische of technische onderwerpen vastgesteld. De Kernenergiewet, het Bbs en de Rbs vormen de basis voor de ANVS-verordening.

In deze handreiking behandelen we de beveiligingsparagraaf 4.3.4 (artikel 4.13 tot en met 4.20) van de ANVS-verordening. In het volgende hoofdstuk gaan we hier nader op in.

3.3. BRAS is en blijft maatwerk

In de groep van honderden vergunninghouders zitten grote verschillen. Denk bijvoorbeeld aan verschillen bij het fabriceren, opslaan, gebruiken en overbrengen van radioactieve stoffen. Daarnaast zijn de omstandigheden van de toepassingen van de radioactieve stoffen verschillend, zoals in ziekenhuizen (open bronnen bij nucleaire geneeskunde) of industrie (gesloten bronnen bij meet- en regeltechniek). Ook binnen één type toepassing zijn er verschillen denkbaar, zoals in vaste meetopstellingen of op wisselende plaatsen. Dat betekent dus ook dat deze verschillen leiden tot variaties in het toepassen van beveiligingsmaatregelen en -voorzieningen. BRAS is en blijft maatwerk. Daarom is naast de expertise van de beveiligingsverantwoordelijke ook die van de stralingsbeschermingsdeskundig en overige experts essentieel bij het opstellen van een beveiligingsplan.

4 Wat staat er in beveiligingsparagraaf 4.3.4 van de ANVS-verordening?

4.1. Beveiliging van de radioactieve stoffen

In beveiligingsparagraaf 4.3.4 van de ANVS-verordening staan de eisen aan de beveiligingsmaatregelen die een vergunninghouder moet nemen. In hoofdstuk 6 van deze handreiking is de precieze tekst en een toelichting op alle artikelen uit de ANVS-verordening te vinden.

4.2. Waar komt de inhoud van deze beveiligingsparagraaf 4.3.4 in het kort op neer?

4.2.1. Persoonlijk of elektronische toezicht tijdens werken (Art 4.14)

Beveiligingsparagraaf 4.3.4 gaat over beveiliging en legt uit dat er altijd persoonlijk of elektronisch toezicht moet zijn op het werken met radioactieve stoffen. De personen die met deze stoffen werken, zijn persoonlijk verantwoordelijk voor de beveiliging ervan. Uiteraard is deze persoonlijke verantwoordelijkheid proportioneel ingericht. Een medewerker hoeft de radioactieve stoffen niet ten koste van alles en iedereen te bewaken. Wel wordt verwacht dat een medewerker de radioactieve stoffen niet onbeheerd achterlaat en dat medewerkers elkaar aanspreken op onveilig gedrag (als bij voorbeeld een collega zich niet aan de procedure en regels houdt). Ook moet de medewerker toezicht houden op de aanwezigheid van de radioactieve stoffen en onbevoegden aanspreken en indien nodig wegsturen. Kortom: voor deze aangewezen persoonlijke toezichthouders is een duidelijke beveiligingstaak neergelegd in beveiligingsparagraaf 4.3.4 van de ANVS-verordening. Het is van belang dat in het beveiligingsplan een opsomming te vinden is van de personen die zijn aangewezen om persoonlijk toezicht te houden of dat er een functieomschrijving is opgenomen. Onderstaande tabel geeft een overzicht van de verschillende toezichtssituaties en welke maatregelen nodig zijn.

	Persoonlijk toezicht	**Elektronisch toezicht**
Hoe	Door de medewerkers die met de radioactieve stoffen werken of beveiligers	Door middel van elektronische detectie en vertraging
Wat	• Radioactieve stoffen niet onbeheerd achterlaten • Onbevoegde personen aanspreken en indien nodig wegsturen • Bij een poging tot een kwaadwillende actie de politie waarschuwen	• Een poging tot diefstal en/of onbevoegde toegang detecteren • Reactie door bewakingsdienst of eigen personeel • Alarm verifiëren • Politie waarschuwen
Uitvoering	• Aanwijzen van diegenen die persoonlijk toezicht dienen te houden door de beveiligingsdeskundige. • Instructie aan deze personen	• Elektronische detectie aanleggen • Vertraging realiseren met deuren, kasten, sloten e.d. • Afspraken maken met een bewakingsdienst

	Persoonlijk toezicht	Elektronisch toezicht
		• Politie vooraf op de hoogte stellen van de risicovolle stoffen die worden opgeslagen

Tabel 1. Persoonlijk en elektronisch toezicht volgens de beveiligingsparagraaf 4.3.4 van de ANVS-verordening

4.2.2. Veilige opslag en beveiliging indien er niet meer gewerkt wordt met de radioactieve stoffen (Art 4.18)

De radioactieve stoffen moeten veilig opgeborgen worden in een daarvoor geschikte opslag of bunker wanneer er niet meer mee gewerkt wordt. Beveiliging kan zowel elektronisch als persoonlijk geregeld worden. Het elektronisch toezicht bestaat uit elektronische detectie in combinatie met vertraging van de dader. Dat betekent dat nadat de elektronische beveiliging is afgegaan het niet mogelijk moet zijn dat een kwaadwillend persoon meteen met de radioactieve stoffen kan weglopen. Deze persoon of personen moeten afdoende vertraagd worden in hun acties zodat er voldoende tijd is voor de responseorganisatie om tijdig ter plaatse te zijn.

Door een plattegrond in het beveiligingsplan op te nemen wordt de ruimtelijke samenhang tussen de beveiligingsmaatregelen weergeven. Ook geeft een plattegrond inzicht in de mogelijke aanvalsroutes van een kwaadwillende.
Geef op de plattegrond in ieder geval aan:

- De ruimtes waar de radioactieve stoffen worden opgeslagen en/of gebruikt;
- De categorieën van de radioactieve stoffen per ruimte, als er binnen de locatie radioactieve stoffen worden opgeslagen of gebruikt die in verschillende categorieën moeten worden ingedeeld;
- De compartimentering of beperkende maatregelen tegen het meenemen van radioactieve stoffen;
- De vertragende bouwkundige maatregelen;
- De vertraging die wordt gerealiseerd langs een bepaalde schil, indien van toepassing;
- De gebruikte elektronische inbraakdetectoren.

Door het uitvoeren van een tijdpadanalyse kan worden vastgesteld of de beveiliging effectief is (zie ook bijlage C). Hiervoor geldt overigens dat de mate van de vereiste vertraging afhankelijk is van het potentieel effect van de radioactieve stoffen, zoals die wordt voorgeschreven in de beveiligingsparagraaf 4.3.4. De stralingsbeschermingsdeskundige informeert de beveiligingsverantwoordelijke over het potentieel effect van de radioactieve stoffen. Bovendien dient een elektronische melding eerst geverifieerd te worden om er zeker van te zijn dat het geen valse melding betreft. Deze alarmverificatie kan door een eigen medewerker uitgevoerd worden. Ook kan daarvoor gebruik gemaakt worden van een ingehuurde bewakingsdienst of van videobeelden die de eigen beveiliging op afstand kan bekijken. Door het uitvoeren van een tijdpadanalyse kan worden vastgesteld of de beveiliging effectief is.

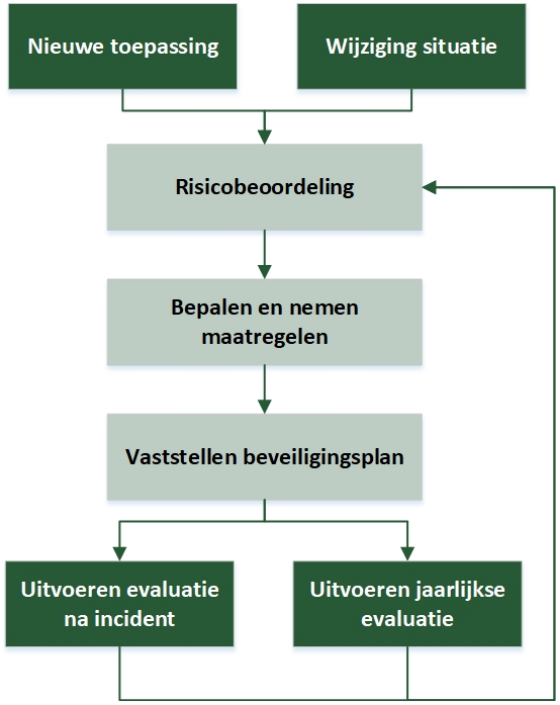
4.2.3. Uitzondering op persoonlijk en elektronisch toezicht

De verdeling in tabel 1 past niet in alle situaties. Als de radioactieve stoffen vastzitten in een industriële installatie is het vaak mogelijk om 24/7 de elektronische detectie aan te laten staan. Het is dan niet nodig om ook persoonlijk toezicht in te richten. Wel is in dat geval van belang dat de bedrijfszekerheid van het toegepaste elektronische toezicht geborgd is met een back-up systeem of door een melding bij een technisch defect. Daarnaast zijn er ook bedrijven die in continue bezetting werken, waardoor er altijd iemand aanwezig is die persoonlijk toezicht houdt. Het staat de vergunninghouder vrij om te kiezen voor de best toepasbare en uitvoerbare oplossing, zolang er altijd persoonlijk of elektronisch toezicht is in combinatie met voldoende vertraging.

5 Processtappen beveiliging radioactieve stoffen

5.1. Het proces van beveiliging van de radioactieve stoffen

Voor de beveiliging van de categorie 1-, 2- of 3-stoffen worden onderstaande stappen gevolgd door de beveiligingsverantwoordelijke.
De stappen uit figuur 1 worden doorlopen wanneer er wordt begonnen met een toepassing waarin beveiliging van de radioactieve stoffen vereist is (nieuwe toepassing) of wanneer de situatie verandert door bijvoorbeeld bouwkundige wijziging of wijziging in de logistiek van de radioactieve stoffen (wijziging situatie).



Figuur 1. stroomschema proces voor de beveiliging van radioactieve stoffen

5.1.1. Risicobeoordeling

Stap één is het maken van een **risicobeoordeling** (Art 4.15 & Art 4.16). Daarin wordt beschreven welk type radioactieve stoffen het betreft, hoe deze worden gebruikt en op welke locatie, waarna de potentiële scenario's worden doorlopen (zie ook bijlage C.). Daarna is het nuttig te bepalen welk daderprofiel (zie § 5.1.2) van toepassing is en hoe een mogelijke interne dreiging eruit kan zien.

5.1.2. Bepalen en nemen van maatregelen

Na het opstellen van een risicobeoordeling, worden de **maatregelen** (Art 4.16) vastgesteld. Dit zijn maatregelen op verschillende vlakken: bouwkundig, elektronisch en organisatorisch. Om eigen medewerkers te informeren, die zelf niet

deskundig zijn op het gebied van stralingsbescherming, is het nuttig om in het beveiligingsplan een korte toelichting te geven van de toepassing van de radioactieve stoffen en de wijze waarop zij worden opgeslagen.

5.1.3. Vaststellen beveiligingsplan

Vervolgens wordt er een **beveiligingsplan** (Art 4.18) vastgesteld waarin de risicobeoordeling en de maatregelen zijn opgenomen, inclusief de contacten met de politie en andere hulpverleningsdiensten.

5.1.4. Evaluatie

Als laatste wordt er een **evaluatie** (Art 4.20) uitgevoerd. Het doel van het evaluatieprogramma is om de beveiligingsmaatregelen na te lopen en te controleren of ze nog functioneren. Kortom: zijn alle beveiligingsmaatregelen uit het beveiligingsplan nog aanwezig en doeltreffend genoeg? Dit evaluatieprogramma dient jaarlijks en na elk beveiligingsincident te worden uitgevoerd.

In de volgende paragrafen volgt een uitgebreidere beschrijving van de onderdelen uit figuur 1. Zo staat in paragraaf 5.2 (risicobeoordeling) een toelichting op de artikelen die van toepassing zijn op dit onderwerp. Daarna volgen respectievelijk de onderwerpen: de te nemen maatregelen en tot slot het opstellen van een beveiligingsplan en de evaluatie.

5.2. Risicobeoordeling

5.2.1. Vaststellen van risicoprofielen (Art 4.15 en 4.16)

Voor een volledige risicobeoordeling moet u systematisch bekijken welke daderprofielen voor uw onderneming relevant zijn. Op welke wijze kunnen deze potentiële daders de onderneming en de maatschappij schaden? U maakt een inschatting van de kans dat zich een incident voordoet en wat dan de schade zou zijn. Zo'n analyse is nuttig omdat het goed inzicht geeft in de te beschermen belangen en in de prioritering van de verschillende beveiligingsmaatregelen.

5.2.2. Daderprofielen

Afhankelijk van het type onderneming en de omgeving waarin deze gevestigd is, zijn verschillende daderprofielen relevant. Hieronder ziet u een aantal voorbeelden van daderprofielen:

- Baldadige jeugd die vanuit een aanvankelijke spelsituatie overschakelt naar baldadig gedrag. Hier is het wegnemen van goederen meestal niet direct het doel.
- Activistische dader die door het verstoren van bedrijfsactiviteiten een bepaald maatschappelijk doel wil bereiken. Bijvoorbeeld het imago aantasten van het bedrijf of de sector.
- Amateur of gelegenheidsinbreker die door de geboden gelegenheid of omstandigheden komt tot het plegen van een misdrijf als er een lage pakkans bestaat.
- Eigen medewerkers of externe medewerkers die uit onvrede of opportunisme bedrijfsmiddelen stelen, hulp bieden aan criminele vrienden van buiten of onder druk worden gezet tot een kwaadwillende actie.
- Crimineel persoon waarvan het inkomen meestal geheel of gedeeltelijk bestaat uit opbrengsten van strafbare activiteiten. Dit type dader neemt meer risico's dan een amateur en beschikt over gespecialiseerd gereedschap.
- Terroristische dader die vanuit ideologische motieven schade probeert toe te brengen, maar niet uit is op geldelijk gewin.

5.2.3. Interne dreiging (Art 4.17)

Nieuw in de beveiligingsparagraaf 4.3.4 is het daderprofiel 'eigen medewerker'. Dit komt voort uit een veranderend dreigingsprofiel. Diefstal, in algemene zin, door het eigen personeel komt helaas in veel bedrijven voor en hierdoor was het nodig deze verplichting op te nemen. Van de vergunninghouder wordt daarom nu ook verwacht dat er maatregelen worden genomen om het risico van diefstal door eigen medewerkers en externe medewerkers zoveel mogelijk te beperken.

Het risico dat wordt gevormd door het eigen personeel is heel anders dan het risico dat inbrekers vormen. In tegenstelling tot inbrekers, heeft het eigen personeel vaak ongehinderd toegang tot de radioactieve stoffen, is op de hoogte van beveiligingsmaatregelen en kan tot op zekere hoogte ongemerkt ongewenste handelingen verrichten. De maatregelen die genomen worden zijn daarom ook heel anders van aard dan de maatregelen tegen inbraak, zoals die in de VRKI worden besproken. Ze hebben meer gemeen met de maatregelen die vanuit het oogpunt van veiligheid worden genomen om het personeel tegen gezondheidsschade door straling te beschermen.

Maatregelen bij interne dreiging

De maatregelen die een vergunninghouder dient te nemen om te beveiligen tegen diefstal of misbruik door eigen personeel, zijn sterk afhankelijk van de aard van de onderneming en van de handelingen die met de radioactieve stoffen worden verricht. Bij bronnen in vaste opstellingen ligt het voor de hand dat het toegangsbeheer tot de ruimte of installatie waar de bronnen zich bevinden een belangrijke maatregel is. Bij mobiele bronnen zal daarnaast ook aandacht moeten worden gegeven aan de beveiliging op het moment dat de bronnen zich buiten de opslag of zelfs buiten het bedrijf bevinden. Ondanks dat het moeilijk is een algemene set maatregelen te beschrijven die op alle ondernemingen van toepassing zijn, worden hierna een aantal mogelijke maatregelen besproken. Dit zijn hoofdzakelijk organisatorische maatregelen:

- Specifieke toegang bij werkzaamheden: als de radioactieve stoffen door meerdere medewerkers worden gebruikt dan is het niet wenselijk dat zij allemaal doorlopend toegang hebben tot die stoffen. Een beveiligingsmaatregel kan zijn om de toegang tot de radioactieve stoffen te beperken tot de specifieke medewerkers die hier op enig moment mee moeten werken en die toegang weer in te trekken zodra de handelingen zijn voltooid. Deze maatregel kan uitgewerkt worden in procedures voor een degelijk sleutelbeleid met toegangsbeheer door autorisatie en registratie.
- Vier ogen regel: vanuit veiligheidsoogpunt mogen bepaalde handelingen niet alleen verricht worden. Vanuit beveiligingsoogpunt kan een vier ogen regel een doeltreffende maatregel zijn. Als deze maatregel vanuit bedrijfsvoeringoogpunt niet haalbaar is, moeten worden bezien of het risico dat wordt gevormd door medewerkers die alleen over een radioactieve stof kunnen beschikken op een andere manier kan worden gecompenseerd.
- Elektronische detectie: elektronische detectie kan ook tijdens werktijd worden ingeschakeld om onbevoegde toegang te detecteren. Ook kunnen in bepaalde industriële processen onbevoegde handelingen via de procesbewaking worden gesignaleerd.
- Beveiligingscultuur: een cultuur van beveiligingsbewustzijn is van belang om het risico op diefstal en misbruik door zowel een kwaadwillende van buiten als eigen medewerkers te verkleinen. De vergunninghouder dient in de instructie aan zijn personeel deze cultuur te bevorderen.

- Zorgvuldige uitdiensttreding: bij het uitdiensttreden van een medewerker dienen zijn autorisaties te worden ingetrokken en zijn toegangspassen en sleutels te worden ingenomen. Ook dienen toegangscodes te worden gewijzigd. Daarnaast helpen procedures bij het uitdiensttreden als het voeren van een exitgesprek, en het ondertekenen van een geheimhoudingsverklaring, ook.
- Opdeling van handelingen: handelingen die nodig zijn om toegang te krijgen tot de radioactieve stoffen worden indien mogelijk verdeeld over meerdere personen, zodat niemand zelfstandig zichzelf toegang kan verschaffen.
- Inschakelen elektronische detectie: Als de elektronische detectie niet op vooraf vastgestelde tijden wordt ingeschakeld, moet dit tot een melding bij de bewakingsdienst en een reactie leiden.
- Beperkte toegang: de vergunninghouder moet in kaart brengen welke medewerkers toegang hebben tot de radioactieve stoffen en deze groep zoveel mogelijk beperken. Hierbij moet naast de medewerkers die daadwerkelijk met de stoffen werken ook worden gedacht aan schoonmakers, logistiek medewerkers, bewakingsdienst, bedrijfshulpverlening (BHV), etc.
- GPS-tracking: mobiele bronnen kunnen worden voorzien van GPS-tracking zodat afwijking van normale werkwijzen kan worden opgemerkt.
- Inzage in beveiligingsplan: tenslotte vormen eigen medewerkers die inzage hebben in het beveiligingsplan een bijzonder risico. Zij zijn op de hoogte van alle beveiligingsmaatregelen en zien wellicht mogelijkheden om deze te omzeilen. Daarom staat in beveiligingsparagraaf 4.3.4 dat er voor eigen medewerkers bijvoorbeeld de verplichting te beschikken over een geldige Verklaring Omtrent het Gedrag (VOG). Hiermee is de screening van deze medewerkers een absoluut minimale basisvoorwaarde.

5.3. Beveiligingsmaatregelen

Beveiligingsmaatregelen verschillen van aard. Zo zijn er naast organisatorische, bouwkundige, elektronische maatregelen ook maatregelen op het gebied van informatiebeveiliging (Art 4.18).

5.3.1. Organisatorische maatregelen

Wat de organisatorische maatregelen betreft worden in ieder geval de procedures en werkinstructies verwacht die helpen het risico op diefstal of misbruik te beperken. Denk bijvoorbeeld aan het sleutelbeheer, het in- en uitschakelen van de alarminstallatie, het houden van persoonlijk toezicht, een sluitronde lopen of het verlenen van autorisatie. Ook procedures die zijn ontworpen om het risico op diefstal door eigen personeel te beperken horen hierbij. Daarnaast moeten er ook procedures zijn die gevolgd moeten worden als zich een (poging) tot diefstal of misbruik voordoet. Denk hierbij aan het alarmeren van de politie en of het waarschuwen van eigen medewerkers. Het is niet nodig alle procedures werkelijk op te nemen in het beveiligingsplan. Een verwijzing in het beveiligingsplan naar de vindplaats ervan is voldoende.

5.3.2. Bouwkundige maatregelen

Met de bouwkundige maatregelen wordt over het algemeen de nodige vertraging behaald bij een poging tot diefstal of misbruik. Het is handig om deze maatregelen zoveel mogelijk in de vorm van prestatie-eisen op het gebied van braakwerend vermogen te beschrijven. Dan is het bij bouwkundige wijzigingen duidelijk welke eisen er aan bepaalde componenten worden gesteld en het geeft de mogelijkheid

om in een verschillende situaties de meest geschikte oplossingen te kiezen. Beschrijf de prestatie-eisen die worden gesteld aan deuren, hang- en sluitwerk, wanden en plafonds en vloeren en aan bijzondere maatregelen zoals tralies of braakwerende kasten.

5.3.3. Elektronische maatregelen

Elektronische maatregelen kunnen verschillende doelen dienen. Het meest relevant voor de beveiliging zijn de systemen die toegang verlenen aan geautoriseerde medewerkers en de systemen die onbevoegden detecteren, zoals beveiligingscamera's en bewegingsmelders. Beschrijf het algemene ontwerp van de systemen en hoe daarvan gebruik wordt gemaakt. Bedenk dat elke bouwkundige vertraging pas ingaat na eerste detectie. Op dat moment gaat de vereiste vertragingstijd lopen.

5.3.4. Informatiebeveiligingsmaatregelen

Onder informatiebeveiligingsmaatregelen wordt bijvoorbeeld het beschermen en compartimenteren van het eigen computernetwerk tegen het binnendringen van buitenaf (hacken) verstaan. Ook gaat het om het beschermen van gevoelige informatie door het op te bergen in een kluis, maar ook het voorkomen van hacken van elektronische sloten en misbruik maken van goed vertrouwen (social engineering) van de medewerkers.

De beveiligingsmaatregelen moeten uiteraard wel met elkaar in verband staan en er moet voorkomen worden dat deze elkaar tegenwerken. Het heeft weinig zin om een deur te voorzien van zwaar hang- en sluitwerk (bouwkundige maatregel) en die deur vervolgens niet op slot te doen (organisatorische maatregel). Door de juiste combinatie te maken tussen deze organisatorische, bouwkundige, elektronische en informatiebeveiliging maatregelen komt u tot een adequaat beveiligingssysteem.

5.3.5. BORG Certificering

U kunt de kwaliteit van de beveiliging aantonen met een BORG-Beveiligingscertificaat. Dit is echter geen verplichting. Het BORG-Beveiligingscertificaat zegt niet alleen iets over de kwaliteit van de toegepaste beveiligingscomponenten en de manier waarop ze zijn verwerkt, maar vooral ook over de samenhang en het beveiligend vermogen ervan. Een BORG-Beveiligingscertificaat wordt alleen uitgereikt als alle volgens de bepaalde beveiligingsklasse vereiste beveiligingsmaatregelen zijn uitgevoerd of daaraan gelijkwaardig zijn.

5.4. Beveiligingsplan

De vergunninghouder van radioactieve categorie 1-, 2-, of 3-stoffen moet op grond van artikel 4.7 van het Besluit basisveiligheidsnormen stralingsbescherming een beveiligingsplan hebben. De ANVS toetst de opzet en inhoud van dat beveiligingsplan. In een beveiligingsplan worden de beveiligingsmaatregelen en de beschrijving van de beveiligingsorganisatie vastgelegd.

De vergunninghouder handelt naar wat is vastgelegd in dit plan en daarop wordt toegezien door de ANVS. Het beveiligingsplan is afgestemd op de aard van de onderneming. Naarmate de diversiteit en activiteit van de radioactieve stoffen, de complexiteit van de organisatie en de beveiligingsmaatregelen toenemen, zal dit ook zijn weerslag hebben in het beveiligingsplan. Dat betekent dus dat ondernemingen met enkelvoudige handelingen en een beperkt gebruik van radioactieve stoffen kunnen volstaan met een beperkter beveiligingsplan. Wel blijft de systematiek in

alle gevallen hetzelfde. Alle artikelen van de beveiligingsparagraaf 4.3.4 moeten dus worden opgenomen in uw beveiligingsplan.

5.4.1. Inhoudelijke eisen beveiligingsplan

Aan het beveiligingsplan worden in de beveiligingsparagraaf 4.3.4 onder artikel 4.13 t/m 4.20 van de ANVS-verordening bepaalde inhoudelijke eisen gesteld.

Een beveiligingsplan wordt opgesteld door een op dit vakgebied bekwaam persoon (Art 4.18 lid 4). Daarnaast is ook de betrokkenheid van de stralingsbeschermingsdeskundige essentieel. Dit is niet verplicht, maar wordt wel zeer aangeraden. Deze samenwerking voorkomt bijvoorbeeld een onjuiste categorie-indeling van de te beveiligen radioactieve stoffen.

5.4.2. Artikelen 4.13 t/m 4.20

Het beveiligingsplan beschrijft de invulling van de artikelen 4.13 tot en met 4.20 van de beveiligingsparagraaf 4.3.4. Het is natuurlijk wel mogelijk dat uw onderneming behoefte heeft aan een meer uitgebreid beveiligingsplan dat ook is geïntegreerd in het managementsysteem dat uw bedrijf hanteert. Dat is uw eigen keuze en verantwoordelijkheid. In ieder geval dienen de artikelen 4.13 t/m 4.20 goed en volledig ingevuld te zijn in dit integraal beveiligingsplan. De beoordeling van het plan wordt door de ANVS gedaan bij een vergunningaanvraag, wijziging of revisie. Daarnaast kan de ANVS bij een inspectie het beveiligingsplan opvragen en toetsen op aanwezigheid van de maartregelen en de werking daarvan. De vergunninghouder moet altijd over een actueel beveiligingsplan beschikken welk voldoet aan de wettelijke verplichtingen.

5.4.3. Beveiligingsplan aanleveren bij vergunningaanvraag

Een beveiligingsplan is verplicht als een ondernemer een vergunning heeft voor het verrichten van handelingen met categorie 1-, 2- of 3-stoffen.

Bij een aanvraag van een nieuwe vergunning, of wijziging (met uitzondering van een administratieve wijziging) of revisie van een bestaande vergunning voor het verrichten van handelingen met categorie 1-, 2- of 3-stoffen, moet een beveiligingsplan ingediend worden. Ook als een wijziging van de vergunning betekent dat de handelingen binnen een categorie vallen en dat daarvoor dit niet het geval was (van nul naar een bepaalde categorie), moet een beveiligingsplan ingediend worden.

Een beveiligingsplan wordt nooit samen met de vergunningaanvraag opgestuurd. Om de vertrouwelijkheid te garanderen dient bij voorkeur het beveiligingsplan per versleutelde e-email naar de digitale postbus (bras@anvs.nl) of desnoods per aangetekende post naar de ANVS verstuurd te worden. Het postadres staat op vindt u via autoriteitnvs.nl/contact.

5.5. Evaluatie

De wijze van evalueren hangt af van de typen maatregelen.

5.5.1. Bouwkundige maatregelen

De **bouwkundige** maatregelen kunnen letterlijk worden nagelopen: sluiten de deuren nog goed, zijn de hekwerken onbeschadigd, et cetera? Maar ook: zijn er verhuizingen of verbouwingen geweest die bestaande bouwkundige maatregelen beïnvloeden? Voor een alarminstallatie wordt vaak een servicecontract afgesloten. De installateur onderhoudt de installatie en geeft een verklaring af dat deze naar

behoren functioneert. Als u geen servicecontract heeft, dient u de installatie zelf te controleren.

5.5.2. Organisatorische maatregelen

Het evalueren van **organisatorische** maatregelen is mogelijk door bijvoorbeeld controle van aftekenlijsten, verificatie van autorisaties, tellen van sleutels en evalueren van incidenten. Wijzigingen in de organisatie kunnen ook effect hebben op de organisatorische beveiligingsmaatregelen en dienen geëvalueerd te worden.

5.5.3. Informatiebeveiligingsmaatregelen

Voor wat betreft de **informatiebeveiliging** kan er in de evaluatie gekeken worden naar de fysieke aanwezigheid van vertrouwelijke documenten, logbestanden van computersystemen en de controle van software updates.

5.5.4. Test of oefening

Ook dient er jaarlijks een test of oefening gedaan te worden van de procedures bij mogelijke beveiligingsincidenten. Hoe uitgebreid deze dient te zijn wordt afgestemd op de aard en omvang van uw organisatie. In een kleine onderneming met weinig medewerkers kan in beginsel worden volstaan met een test van de alarmopvolging naar de meldkamer of sleutelhouders. In grotere organisaties, die bijvoorbeeld over een eigen beveiligingsorganisatie en/of een eigen bewakingsdienst beschikken, is een uitgebreidere oefening met deze organisatie of dienst aan de orde.

Uit deze evaluatie kan naar voren komen dat er wijzigingen van maatregelen en/of het beveiligingsplan noodzakelijk zijn. Als dat zo is, dan begint u weer bij de risicobeoordeling zoals beschreven in de grafiek.

In het beveiligingsplan moet ook worden beschreven op welke wijze en wanneer een evaluatie wordt uitgevoerd, wie hiervoor verantwoordelijk is, aan wie de uitkomst gerapporteerd wordt en hoe eventuele verbeterpunten uit de evaluatie zullen worden gemonitord en opgepakt binnen een bepaalde termijn.

6 Toelichting op artikelen beveiligingsparagraaf 4.3.4

In dit hoofdstuk vindt u alle artikelen uit beveiligingsparagraaf 4.3.4 van de ANVS-verordening. In de cursieve tekst wordt artikelsgewijze toelichting (nota van toelichting) van de artikelen uit beveiligingsparagraaf 4.3.4 van de ANVS-verordening gegeven.

Artikel 4.13 (beveiliging tegen diefstal of misbruik van radioactieve stoffen)	
4.13, lid 1	Een vergunninghouder treft de beveiligingsmaatregelen die noodzakelijk zijn om categorie 1-, 2-, of 3-stoffen te beveiligen tegen diefstal of misbruik.
4.13, lid 2	Een vergunninghouder wijst een beveiligingsverantwoordelijke aan voor de toepassing van de beveiligingsmaatregelen, bedoeld in het eerste lid.
In artikel 4.2 van de Regeling basisveiligheidsnormen stralingsbescherming is aangegeven dat voor handelingen met categorie 1-, 2- of 3-stoffen een beveiligingsplan vereist is. In bijlage 4.1 bij de Regeling zijn deze categorieën gedefinieerd. Het eerste lid van artikel 4.2 schrijft voor dat de vergunninghouder beveiligingsmaatregelen voor deze radioactieve stoffen treft. Het tweede lid is een uitwerking van welke persoon op operationeel niveau verantwoordelijk is voor het beveiligingsbeleid. In veel grotere organisaties is het gebruikelijk dat een functionaris wordt aangesteld die operationele verantwoordelijkheid draagt voor de beveiliging. In kleinere organisaties kan deze functie ook als neventaak worden uitgevoerd door een andere functionaris, zoals een stralingsbeschermingsdeskundige of een toezichthoudend medewerker stralingsbescherming. Met het opnemen van de functie van beveiligingsverantwoordelijke wordt in ieder geval beoogd dat deze taken expliciet aan een functionaris worden toegewezen.	

Artikel 4.14 (toezicht op radioactieve stoffen)	
4.14, lid1	Categorie 1-, 2- of 3-stoffen staan permanent onder persoonlijk of elektronisch toezicht.
4.14, lid2	Diegene die persoonlijk toezicht houdt, is hiertoe aangewezen door de beveiligingsverantwoordelijke.
Tijdens handelingen met de radioactieve stoffen is er veelal persoonlijk toezicht door degene die de handelingen verricht. Zij hebben op dat moment de taak ervoor te zorgen dat de radioactieve stoffen niet worden ontvreemd. Dit toezicht kan dus alleen worden verricht door daadwerkelijk persoonlijk aanwezig te zijn. Als er geen handelingen met de radioactieve stoffen worden uitgevoerd is de beveiliging veelal afhankelijk van de combinatie van (elektronische) detectie en bouwkundige vertraging. De eisen aan deze vertraging worden in artikel 4.15 gegeven. Een aantal vergunninghouders heeft professionele beveiligers in dienst of ingehuurd. Deze beveiligers zijn veelal belast met verschillende taken en houden geen persoonlijk toezicht op de radioactieve stoffen. Als zij daarmee wel belast zijn dan dient deze taak expliciet bij hen belegd te zijn en kunnen zij niet tegelijkertijd andere taken uitvoeren. De taken van diegenen die persoonlijk toezicht houden en van de beveiligers worden in het beveiligingsplan beschreven (artikel 4.18, tweede lid, onderdelen e en f, van de ANVS-verordening). Met het tweede lid wordt het aanwijzen van de persoonlijk toezichthouders als operationele taak toebedeeld aan de beveiligingsverantwoordelijke.	

Artikel 4.15 (vertraging bij wederrechtelijke verkrijging van radioactieve stoffen)	
Wanneer categorie 1-, 2-, of 3-stoffen niet onder persoonlijk toezicht staan, zijn de beveiligingsmaatregelen van een vergunninghouder zodanig dat elektronische detectie van een poging tot diefstal of misbruik plaatsvindt en dat vanaf dat moment maatregelen werkzaam zijn die leiden tot:	
a	ten minste 10 minuten vertraging in de tijd die iemand nodig heeft om wederrechtelijk beschikking te krijgen over een categorie 1-stof.
b	ten minste 5 minuten vertraging in de tijd die iemand nodig heeft om wederrechtelijk beschikking te krijgen over een categorie 2-stof.
c	ten minste 3 minuten vertraging in de tijd die iemand nodig heeft om wederrechtelijk beschikking te krijgen over een categorie 3-stof.
Indien (tijdelijk) geen sprake is van persoonlijk toezicht moet er sprake zijn van een combinatie van elektronisch toezicht en bepaalde vertragingstijden. Deze vertragingstijd kan worden omschreven als de tijd in minuten die een potentiële dader nodig heeft om vanaf het moment dat hij wordt gedetecteerd beschikking te krijgen over de radioactieve stof. Immers, vanaf het moment dat de potentiële dader beschikking krijgt over een stof kan hij deze misbruiken. Tijdens gebruik van de radioactieve stoffen is het niet nodig om een vertragingstijd te realiseren. Tijdens gebruik staan de radioactieve stoffen immers constant onder toezicht van degene die de stoffen gebruikt. De vereiste vertragingstijd is afhankelijk van de categorie-indeling van de radioactieve stof. De vertragingstijd is een sommatie van alle factoren die van invloed zijn op de tijd die nodig is om een stof in bezit te krijgen. Naast de vertragingstijd door de getroffen beveiligingsmaatregelen gaat het daarbij bijvoorbeeld om de tijd die de potentiële dader nodig heeft om de afstand tussen de inbraakdetector en de radioactieve stoffen te overbruggen. Door beveiligingsmaatregelen te treffen die de vertragingstijd verlengen, zijn de vergunninghouder en de eventuele bewakingsdiensten of de politie beter in de gelegenheid om de diefstal of het misbruik te voorkomen.	
Zie ook bijlage C van deze handreiking.	

Artikel 4.16 (afstemming beveiligingsmaatregelen)	
De beveiligingsmaatregelen, bedoeld in de artikelen 4.13, 4.14 en 4.15 worden afgestemd op:	
a	de aard van de categorie 1-, 2-, of 3-stof;
b	de manier waarop de categorie 1-, 2-, of 3-stof wordt gebruikt of opgeslagen;
c	de verplaatsbaarheid van de categorie 1-, 2-, of 3-stof;
d	de mogelijke gevolgen voor mensen, dieren, planten en goederen door blootstelling aan ioniserende straling of het vrijkomen van de categorie 1-, 2-, of 3-stof in geval van diefstal of misbruik;
e	de maatregelen die zijn of worden getroffen om de nadelige gevolgen van ioniserende straling voor mensen, dieren, planten en goederen te voorkomen of te beperken.
De vergunninghouder stemt de te treffen beveiligingsmaatregelen af op de factoren genoemd in dit artikel. Bij het realiseren van de vertragingstijd en bij de inrichting van het elektronisch toezicht kan bijvoorbeeld de verplaatsbaarheid van de stof een rol spelen. Ook bij overige beveiligingsmaatregelen ter invulling van de zorgplicht in artikel 4.13, eerste lid, spelen de factoren genoemd in artikel 4.16 een rol. Een voorbeeld is het omhullen van een sterk stralende stof met een moeilijk te verwijderen omhulsel, om zo de kans op het vrijkomen van grote hoeveelheden straling bij diefstal of misbruik te verminderen. Met onderdeel e.	

van artikel 4.16 wordt voorkomen dat beveiligingsmaatregelen zouden leiden tot minder stralingsbescherming.

Artikel 4.17 (beveiliging tegen interne dreigingen)
Een vergunninghouder treft beveiligingsmaatregelen om de gelegenheid tot diefstal of misbruik van de categorie 1-, 2- en 3-stoffen door eigen werknemers of externe werknemers zo veel mogelijk te beperken.
Artikel 4.17 is een nieuw voorschrift op grond van voortschrijdend inzicht en vanwege een veranderend dreigingsprofiel. Met dit artikel wordt een nieuw type dreigingen geïntroduceerd in de verordening. Waar de vergunninghouder voorheen alleen tegen dreigingen van buiten diende te beveiligen, dient hij nu ook tegen dreigingen van binnen te beveiligen. Hiermee wordt met name gedoeld op sabotage of diefstal door het eigen personeel. De vergunninghouder dient dit risico zo veel mogelijk te beperken. De maatregelen dienen proportioneel te zijn ten opzichte van de dreigingen en risico's en het is niet de bedoeling dat dit leidt tot maatregelen die extreem hoge kosten met zich meebrengen. Wel wordt beoogd dat de vergunninghouder meer eenvoudige, voor de hand liggende maatregelen neemt als het risico daarmee aanzienlijk verlaagd kan worden. Voorbeelden zijn het invoeren of formaliseren van een twee-personen regel of het plaatsen van elektronische maatregelen waarmee mobiele bronnen kunnen worden gevolgd.

.

Artikel 4.18 (beveiligingsplan)	
4.18, lid 1	Een vergunninghouder beschikt over een beveiligingsplan met een beschrijving van de wijze waarop de categorie 1-, 2-, of 3-stof wordt beveiligd.
4.18, lid 2	Het beveiligingsplan bevat ten minste een beschrijving van:
a	de categorie-indeling van de te beveiligen radioactieve stoffen overeenkomstig artikel 4.2 van de Regeling basisveiligheidsnormen stralingsbescherming.
b	de manier waarop de categorie 1-, 2-, of 3-stof wordt gebruikt of opgeslagen.
c	een plattegrond van de locatie waarop de plaats waar de categorie 1-, 2-, of 3-stof wordt gebruikt of opgeslagen is aangegeven, alsmede de getroffen beveiligingsmaatregelen.
d	de getroffen en te treffen organisatorische, bouwkundige, elektronische, informatie en andere beveiligingsmaatregelen, waaruit onder andere blijkt hoe met deze maatregelen de in artikel 4.15 bedoelde vertragingstijd wordt behaald.
e	diegenen die aangewezen zijn persoonlijk toezicht te houden als bedoeld in artikel 4.14, tweede lid
f	de taken en bevoegdheden van de personen, belast met de beveiliging van de categorie 1-, 2-, of 3-stof;
g	de procedures die de personen, belast met de beveiliging van de categorie 1-, 2-, of 3-stof moeten volgen, waarbij in ieder geval wordt beschreven hoe zij moeten handelen in geval van diefstal of misbruik van de categorie 1-, 2-, of 3-stof of een poging daartoe.
h	afspraken over de wijze van en mate waarin responsacties van een particuliere beveiligingsdienst worden uitgevoerd of een afschrift van een mededeling aan de politie of veiligheidsregio met betrekking tot de radioactieve stoffen die bij de vergunninghouder zijn opgeslagen.

i	een evaluatieprogramma om de beveiligingsmaatregelen te beoordelen.
4.18, lid 3	Een vergunninghouder handelt in overeenstemming met het beveiligingsplan.
4.18, lid 4	Het beveiligingsplan wordt opgesteld door een op dit vakgebied bekwaam persoon.
Uit inspectieverslagen, voortschrijdend inzicht en een veranderend dreigingsprofiel op het vlak van misbruik, sabotage en ontvreemding van onderhavige bronnen is de oorspronkelijke opzet, inhoud en uitwerking van het beveiligingsplan (inclusief evaluatieprogramma, verantwoordelijkheden etc.) aangescherpt en deels verhelderd. De vakbekwaamheid van degene die het beveiligingsplan op stelt kan blijken uit een opleiding, ervaring of de kwaliteit van het geleverde werk. Het beveiligingsplan kan opgesteld worden door de beveiligingsverantwoordelijke zoals bedoeld in artikel 4.14 of een ander vakbekwaam persoon.	

Artikel 4.19 (inzage beveiligingsplan)	
4.19, lid 1	Een vergunninghouder zorgt ervoor dat van het beveiligingsplan, bedoeld in artikel 4.7 van het besluit, slechts kennis nemen de personen voor wie dit noodzakelijk is voor het goed uitvoeren van hun functie.
4.19,lid 2	Een vergunninghouder zorgt ervoor dat deze personen, alvorens zij kennisnemen van het beveiligingsplan, een verklaring omtrent het gedrag of een verklaring als bedoeld in artikel 1, eerste lid, onderdeel b, van de Wet veiligheidsonderzoeken overleggen die niet ouder is dan vijf jaar.
Ingevolge artikel 4.19 moet de vergunninghouder ervoor zorgen dat slechts diegenen voor wie dat noodzakelijk is voor het uitvoeren van hun functie, kennis nemen van het beveiligingsplan. De geëiste Verklaring Geen Bezwaar (VGB) of Verklaring Omtrent Gedrag (VOG) dient niet ouder dan vijf jaar te zijn.	

.

Artikel 4.20 (uitvoeren evaluatieprogramma)	
4.20, lid 1	Een vergunninghouder voert jaarlijks en na elke inbreuk op de beveiliging het evaluatieprogramma, bedoeld in artikel 4.18, tweede lid, onderdeel i, uit.
4.20, lid 2	Als onderdeel van het evaluatieprogramma worden:
a	de procedures, bedoeld in artikel 4.18, tweede lid, onderdelen g en h, in een oefening getest, en
b	de organisatorische, bouwkundige, elektronische, informatie en andere beveiligingsmaatregelen, als bedoeld in artikel 4.18, tweede lid, onderdeel d, op doelmatigheid beoordeeld en getest.
4.20, lid 3	De bevindingen van het evaluatieprogramma worden op schrift gesteld.
4.20, lid 4	Het uitvoeren van het evaluatieprogramma wordt gebruikt om het beveiligingsbewustzijn binnen de organisatie te verhogen.
4.20, lid 5	Een vergunninghouder wijzigt het beveiligingsplan voor zover de bevindingen van het evaluatieprogramma daartoe aanleiding geven.
Het beveiligingsplan moet actueel worden gehouden en regelmatig worden gecontroleerd en beoordeeld. De uitvoering geschiedt steeds uiterlijk 12 maanden na de vorige evaluatie. Aan de hand van de jaarlijkse evaluatie beoordeelt de vergunninghouder vervolgens of het beveiligingsplan doeltreffend is of aanpassing behoeft	

Bijlage A Referenties en bronnen

ANVS	Algemeen https://www.autoriteitnvs.nl
Bbs	Besluit van 23 oktober 2017, houdende vaststelling van regels ter bescherming van personen tegen de gevaren van blootstelling aan ioniserende straling (Besluit basisveiligheidsnormen stralingsbescherming) https://wetten.overheid.nl/BWBR0040179/2018-07-01
Rbs	Regeling van 15 februari 2019, houdende vaststelling van nadere regels ter bescherming van personen tegen de gevaren van blootstelling aan ioniserende straling (Regeling basisveiligheidsnormen stralingsbescherming) https://wetten.overheid.nl/BWBR0040509/2019-02-15
Vbs	ANVS-verordening basisveiligheidsnormen stralingsbescherming
EU01	Richtlijn 96/29/Euratom van de Raad van 13 mei 1996 tot vaststelling van de basisnormen voor de bescherming van de gezondheid der bevolking en der werkers tegen de aan ioniserende straling verbonden gevaren. http://eurex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0029:NL:HTML
EU02	Council conclusions on strengthening chemical, biological, radiological and nuclear (CBRN) security in the European Union - an EU CBRN Action Plan; 15505/1/09 REV 1. http://register.consilium.europa.eu/pdf/en/09/st15/st15505-re01.en09.pdf
IAEA01	General Safety Requirements Part 3 (Interim). Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards. http://www-pub.iaea.org/MTCD/publications/PDF/p1531interim_web.pdf
IAEA02	Code of Conduct on the Safety and Security of Radioactive Sources; IAEA/CODEOC/2004. http://www-pub.iaea.org/MTCD/publications/PDF/Code-2004_web.pdf http://hps.org/documents/IAEATecDoc1344.pdf
IAEA03	IAEA Nuclear Security Series No. 11, Security of Radioactive Sources. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1387_web.pdf
IAEA04	E P R - D –VALUES 2006, Dangerous quantities of radioactive material (D-values). http://www-pub.iaea.org/MTCD/publications/PDF/EPR_D_web.pdf
IAEA05	Security of nuclear and other radioactive material https://www.iaea.org/publications/12289/planning-and-organizing-nuclear-security-systems-and-measures-for-nuclear-and-other-radioactive-material-out-of-regulatory-control

IAEA06 Preventive and protective measures against insider threats: implementing guide. Vienna : International Atomic Energy Agency, 2008. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1359_web.pdf

MR01 Regeling van de Minister van Economische Zaken van 3 december 2012, nr. WJZ / 12311250, houdende regels inzake de beveiliging van radioactieve stoffen (Regeling beveiliging radioactieve stoffen). http://wetten.overheid.nl/BWBR0032390

VRKI Verbeterde Risicoklassen indeling voor bedrijven; Versie: 2.0; 1 januari 2019. https://hetccv.nl/fileadmin/Afbeeldingen/Certificatie-en-inspectie/Verbeterde_Risicoklassenindeling__VRKI_/VRKI_deel_A_januari_2019.pdf

Bijlage B Categorie-indeling van te beveiligen radioactieve stoffen

De radioactieve stoffen worden op basis van bijlage 4.1 van de Regeling basisveiligheidsnormen stralingsbescherming (Rbs) gecategoriseerd in drie beveiligingsklassen. Hierbij is aangesloten bij de internationaal geaccepteerde systematiek van de IAEA [IAEA03]. Als de radioactieve stoffen niet op basis van deze bijlage kunnen worden gecategoriseerd, dan is voor deze stoffen geen beveiligingsplan vereist en hoeven er geen aanvullende beveiligingsmaatregelen te worden genomen. De vergunninghouder is dan echter nog wel gehouden aan de algemene zorgplicht voor de beveiliging zoals bedoeld in artikel 4.4, derde lid van het Besluit basisveiligheidsnormen stralingsbescherming.

<table>
<tr><th></th><th>Categorie-indeling</th><th>Vertragingstijd</th><th>Beveiligings-eisen</th><th>IAEA security level</th><th></th></tr>
<tr><td rowspan="6">Risico (laag ←→ hoog)</td><td>1</td><td>10 minuten</td><td rowspan="3">ANVS-verordening § 4.3.4 Beveiliging</td><td>A</td><td rowspan="6">Maatregel (licht ←→ zwaar)</td></tr>
<tr><td>2</td><td>5 minuten</td><td>B</td></tr>
<tr><td>3</td><td>3 minuten</td><td>C</td></tr>
<tr><td>4</td><td></td><td rowspan="2">Besluit basisveiligheidsnormen stralingsbescherming, artikel 4.4; Algemene verplichtingen ondernemer</td><td rowspan="2">Basic Safety Standards</td></tr>
<tr><td>5</td><td></td></tr>
</table>

Tabel 2. Vergelijking categorie-indeling en beveiligingsniveaus IAEA

De categorisering gebeurt in eerste instantie op basis van expliciete aanwijzing in de tabel in de bijlage bij de Rbs (Regeling basisveiligheidsnormen stralingsbescherming) [tabel 4]. Dat wil zeggen dat als er in de vergunning met naam een toepassing wordt genoemd en deze toepassing staat in de tabel, dat hiermee de categorie bepaald moet worden. Als er niet gecategoriseerd kan worden door expliciete aanwijzing, dan moet de categorie bepaald worden op basis van de A/D waarde.
De 'A' in A/D waarde staat voor de activiteit van de radioactieve stof. Hierbij moet worden uitgegaan van de vergunde activiteit, niet van de activiteit die op een bepaald moment op aanwezig is. De 'D' staat voor een 'D-waarde'. Dit is de activiteit die volgens het IAEA een gevaarlijke hoeveelheid oplevert. Deze activiteiten zijn te vinden in het IAEA document 'Dangerous quantities of radioactive material' [IAEA04]. Door A te delen door D krijgen ontstaat een beeld van hoe gevaarlijk de vergunde activiteit is. In deze berekening dienen A en D in dezelfde eenheid uitgedrukt te worden. Voor de D-waarden is dat TeraBecquerel (TBq). Als A/D = 1, dan is er sprake van één keer de gevaarlijke hoeveelheid, wat betekent dat de radioactieve stof in categorie 3 valt. Als A/D = 10, dan is er sprake van tien keer de gevaarlijke hoeveelheid en komt de indeling uit op categorie 2. Als A/D = 1000, dan is er sprake van duizend keer de gevaarlijke hoeveelheid en geldt categorie 1.

Als de ondernemer een vergunning heeft voor meerdere radioactieve stoffen, dan maakt het voor de categorie-indeling uit of de stoffen in één ruimte worden opgeslagen of dat ze verspreid worden over verschillende ruimten. De categorie indeling wordt namelijk per ruimte bepaald. Let op: ook hier moet worden uitgegaan van wat er per ruimte is vergund of is aangevraagd, niet van wat er daadwerkelijk aanwezig is. Daarnaast maakt het uit of er per radioactieve stof beveiligingsmaatregelen genomen zijn of dat de stoffen gezamenlijk zijn beveiligd. Een beveiligingsmaatregel die per radioactieve stof genomen kan worden, is bijvoorbeeld een ketting waarmee een bronhouder verankerd wordt aan het gebouw. Als er dergelijke maatregelen genomen zijn kan de categorie bepaald worden per radioactieve stof en niet per ruimte. Zo niet, dan moet er worden uitgegaan van de verzamelde radioactieve stoffen in de ruimte.

Om de categorie van een verzameling radioactieve stoffen te bepalen, zijn twee punten van belang. Ten eerste wordt bekeken of de radioactieve stoffen gecategoriseerd kunnen worden op basis van expliciete aanwijzing. Ten tweede wordt beoordeeld welke categorie geldt als de A/D waarde wordt uitgerekend van de gesommeerde activiteiten van alle aanwezige radioactieve stoffen. Vervolgens wordt de categorie-indeling gekozen met de laagste cijferaanduiding en dus de zwaarste beveiligingsklasse.

De gesommeerde A/D-waarde wordt daarbij bepaald volgens de formule:

$$\frac{A}{D} = \sum_{n} \frac{\sum_i A_{i,n}}{Dx_n}$$

Eerst wordt dus voor elk nuclide de voor de ruimte vergunde activiteit opgeteld en gedeeld door de D-waarde van dat nuclide. Dit geeft de A/D waarde per nuclide. Vervolgens worden de A/D waarden van alle voor die ruimte vergunde nucliden opgeteld. Dit geeft de gesommeerde A/D waarde. Door op deze manier de categorie te bepalen, wordt altijd voor de zwaarste beveiligingsmaatregelen gekozen voor de radioactieve stoffen die volgens de vergunning in een ruimte aanwezig kunnen zijn.

Bijlage C Tijdpadanalyse

Door het uitvoeren van een analyse kan worden vastgesteld of de beveiliging effectief is. Een analyse begint altijd met het beschrijven van de beveiligingsmaatregelen, zodat duidelijk is hoe de beveiligingsmaatregelen met elkaar in verband staan. Ook is het nodig te bedenken hoe een kwaadwillende zijn slag zou kunnen proberen te slaan. Welke routes kan hij lopen door het pand en welke deuren of ramen moet hij dan forceren? Waar is de detectie geplaatst en wanneer wordt een kwaadwillende gedetecteerd? In complexe situaties kan het nodig zijn om hiervoor verschillende deelscenario's vast te stellen. In eenvoudigere gevallen volstaat het vastleggen van de meest waarschijnlijke route en is het voldoende om een enkel - tijdig - detectiemoment vast te stellen.

Op basis van artikel 4.18 van de ANVS-verordening is het uitvoeren van een analyse verplicht en dient de ondernemer aannemelijk te maken dat de genomen maatregelen in samenhang de vereiste vertraging na detectie kunnen garanderen. De analyse is alleen verplicht voor het scenario 'diefstal buiten handelingen' en niet voor het scenario 'diefstal tijdens handelingen' omdat de radioactieve stoffen dan onder persoonlijk toezicht dienen te staan. Ook wordt met deze analyse gedoeld op een beroepsinbreker als dader en niet een eigen medewerker.

Scenario	Toezicht	Prestatie eis	
Diefstal of misbruik door crimineel tijdens handelingen	Persoonlijk toezicht	Voor zo ver als redelijk mogelijk voorkomen	
Diefstal of misbruik door crimineel buiten handelingen	Elektronisch Vertraging	Effectief 3, 5 of 10 minuten	→ Analyse
Diefstal of misbruik door eigen medewerker tijdens handelingen	Persoonlijk toezicht	Gelegenheid zoveel mogelijk beperken	
Diefstal of misbruik door eigen medewerker buiten handelingen	Elektronisch Vertraging	Gelegenheid zoveel mogelijk beperken	

Tabel 3. Scenario waarvoor analyse verplicht is

De meest voor de hand liggende, effectieve vorm is dat te doen met een tijdpadanalyse. De getroffen beveiligingsmaatregelen worden uitgezet op een tijdlijn waarbij wordt uitgegaan van het detectiemoment, de vertraging die door de genomen beveiligingsmaatregelen wordt gerealiseerd, maar ook de tijd die een dader nodig heeft bepaalde routes af te leggen. Uit dit deel van de analyse blijkt in ieder geval hoeveel een dader wordt vertraagd nadat hij gedetecteerd is en voordat hij er met radioactieve stoffen vandoor kan gaan. Als er meerdere deelscenario's zijn gedefinieerd, moet voor elk deelscenario een analyse worden gemaakt.

De tijdlijn kan worden aangevuld met een tweede lijn waarop de alarmering en respons van de bewakingsdienst en/of de politie is uitzet. Deze twee tijdlijnen worden dan vervolgens met elkaar vergeleken en hieruit kan worden geconcludeerd

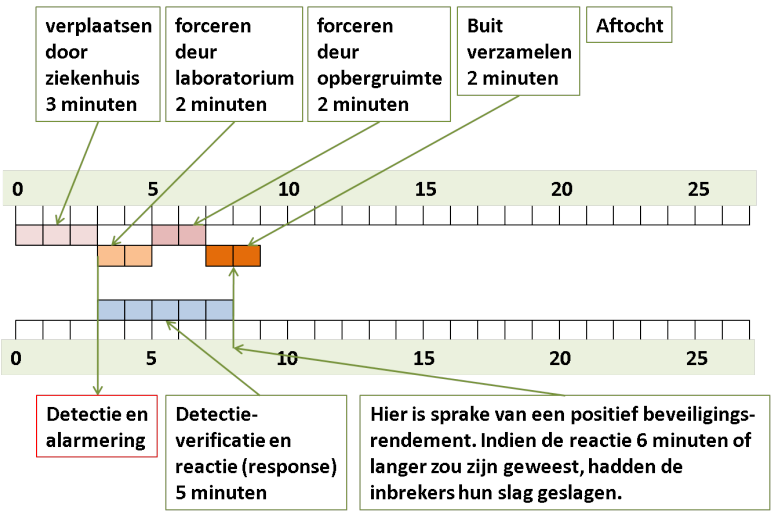
of er sprake is van een positief of negatief beveiligingsrendement: is er sprake van tijdige detectie van de kwaadwillende of niet? Dit tweede deel van de analyse is in de regelgeving niet verplicht gesteld, maar het spreekt voor zich dat een analyse zonder dit deel eigenlijk niet compleet is.

Net zoals de eerste tijdlijn start de tweede tijdlijn ook altijd met het cruciale detectiemoment. Dit is over het algemeen een elektronisch alarm. Op het moment van afgaan is het vaak nog niet zeker dat er daadwerkelijk een inbraak plaatsvindt. Elektronische alarmsystemen geven helaas soms valse meldingen. Ook kan er een alarm afgaan doordat een eigen medewerker vergeten is het alarm uit te schakelen. Het alarm moet daarom eerst geverifieerd worden voordat de politie kan worden gewaarschuwd. Deze alarmverificatie kan worden verricht door een bewakingsdienst ter plaatse te sturen of door gebruik te maken van camera's.

Nadat het alarm is geverifieerd en de politie of de particuliere bewakingsdienst is gewaarschuwd, duurt het nog enige tijd voordat zij ter plaatse zijn. Alleen als de politie of de particuliere bewakingsdienst op tijd ter plaatse is om de daders op heterdaad aan te houden is er sprake van een positief beveiligingsrendement.

Voorbeeld

De volgende casus werkt dit uit en maakt één en ander duidelijk. De casus betreft de diefstal uit een laboratorium van een ziekenhuis. Voor deze casus is gekozen voor een beknopt scenario d.m.v. directe doormelding en onmiddellijke opvolging. In de praktijk zal een tijdpadanalyse meerdere stappen bevatten



Stel: een dader heeft zijn zinnen gezet op goederen die hij in een laboratorium van een ziekenhuis heeft zien staan. Om in dat laboratorium te komen, moet hij zich door het ziekenhuis verplaatsen. Vervolgens moet hij de deur van het laboratorium forceren om binnen te komen. Daarna is de deur van de opbergkast aan de beurt. De radioactieve stoffen liggen voor het grijpen, hij verzamelt deze en start vervolgens de aftocht. Deze handelingen nemen in totaal negen minuten in beslag.

Op het moment dat hij de eerste deur forceert, wordt een detector geactiveerd. Dat moment van 'tijdige' detectie is cruciaal in het beveiligingsconcept van elke onderneming. De tijd tussen alarmering en de start van de aftocht is de vertragingstijd. De detector genereert een alarm dat in de portiersloge bij de ingang van het ziekenhuis ontvangen wordt. Eén van de beveiligingsbeambten krijgt opdracht om op locatie poolshoogte te gaan nemen. Als blijkt dat het een

daadwerkelijk (en dus geen vals) alarm is, is het mogelijk dat hij de dader (op heterdaad) aanhoudt, of dat hij via de portiersloge de politie waarschuwt. In dat laatste geval gaat de politie na ontvangst van de melding van het ziekenhuis met spoed ter plaatse en betrapt zo mogelijk de dader (op heterdaad).

Bijlage D Kernenergiewet, Bbs en Rbs

Kernenergiewet

De Kernenergiewet is een raamwet waarin bevoegdheden voor de Rijksoverheid, mogelijkheden voor nadere wetgeving en een stelsel van vergunningen zijn opgenomen. Het voornaamste doel van deze wet is het beschermen van milieu, werknemers en bevolking tegen de schadelijke gevolgen van ioniserende straling. Aan de wet zijn tal van Algemene Maatregelen van Bestuur (AMvB of besluit) en Ministeriële Regelingen (MR of regeling) gekoppeld, die invulling geven aan voorschriften voor het werken met bronnen van ioniserende straling.

Besluit basisveiligheidsnormen stralingsbescherming (Bbs)

Het Besluit basisveiligheidsnormen stralingsbescherming (Bbs) is een Algemene Maatregel van Bestuur (AMvB), die een verdere invulling geeft van de Kernenergiewet. Het besluit beschermt verschillende groepen die te maken hebben met ioniserende straling: werknemers, patiënten, bevolking en het milieu.
De regels uit het Bbs zorgen ervoor dat bevolking, het milieu, medewerkers en patiënten nu en in de toekomst beschermd zijn tegen de gevolgen van ioniserende straling. In de regels staat onder andere het volgende:

- Mensen die werken met stralingsbronnen worden goed beschermd. Er gelden hoge eisen aan het controlesysteem. Belangrijk bij dit controlesysteem is: hoe hoger het risico, des te strenger de eisen en het toezicht zijn.
- Er gelden strenge grenswaarden voor vrijstelling en vrijgave van radioactieve stoffen, die vrijkomen na bijvoorbeeld grondboringen of een behandeling in een ziekenhuis. Deze grenswaarden zijn wereldwijd hetzelfde.
- De voorschriften voor de stralingsbeschermingsdeskundige en toezichthoudend medewerker stralingsbescherming binnen de Europese Unie zijn gelijk. Deze deskundigen zorgen voor het veilig werken met straling, bijvoorbeeld in ziekenhuizen en bedrijven.
- Sommige ondernemers zijn verplicht om een ‘standaard vergunning’, een registratie, voor het gebruik van een stralingsbron te doen. De registratie geldt voor het grootste deel van de röntgenapparaten van tandartsen en dierenartsen.
- Andere ondernemers zijn verplicht om een vergunningaanvraag in te dienen voor het werken met een stralingsbron. Voor deze vergunningsaanvraag moet de ondernemer informatie aanleveren zoals: een omschrijving van het onderhoud en het inspectieprogramma van apparatuur of contracten voor de terugname van sommige radioactieve bronnen.
- Bedrijven die werken met een bepaalde radioactieve stof moeten een beveiligingsplan hebben. In dit plan staat bijvoorbeeld verplicht beschreven hoe een bedrijf omgaat met diefstal door eigen personeel.

Artikel 4.7 van het Bbs schrijft voor dat de vergunninghouder dient te beschikken over een beveiligingsplan waarin de beveiligingsmaatregelen zijn beschreven. Deze verplichting geldt voor alle houders van een vergunning voor radioactieve stoffen die op basis van de tabel in bijlage 4.1 bij de Regeling basisveiligheidsnormen stralingsbescherming kunnen worden ingedeeld.

Artikel 4.7. (beveiliging radioactieve stoffen)

1. De ondernemer zorgt in gevallen, behorend tot een bij regeling van Onze Minister aangewezen categorie, voor een beveiligingsplan waarin wordt beschreven welke voorzieningen met betrekking tot de beveiliging van een bron zijn getroffen.

2. De aanwijzing, bedoeld in het eerste lid, staat in een passende verhouding tot de aard en zwaarte van de betrokken risico's, overeenkomstig de graduele benadering, bedoeld in artikel 1.1. Bij verordening van de Autoriteit kunnen afhankelijk van de aard en zwaarte van de betrokken risico's, eisen aan de vorm, inhoud en kwaliteit van het beveiligingsplan en de wijze van uitvoering ervan worden gesteld. Deze eisen kunnen een plicht tot rapportage aan de Autoriteit omvatten.

3. Bij verordening van de Autoriteit kunnen in het belang van de stralingsbescherming en beveiliging nadere regels worden gesteld ten aanzien van het beveiligingsplan en de beveiliging van het voorhanden hebben van radioactieve stoffen, bestemd voor handelingen waarvoor krachtens de wet of dit besluit een vergunning is vereist.

Regeling basisveiligheidsnormen stralingsbescherming (Rbs)

Op woensdag 10 januari 2019 publiceerde de Staatscourant de ministeriële regeling basisveiligheidsnormen stralingsbescherming (Rbs). Dit besluit vervangt de eerdere ministeriële regeling en is een uitwerking van het Besluit basisveiligheidsnormen stralingsbescherming dat op 6 februari 2018 in werking is getreden. In artikel 4.2 wordt de aanwijzing gegeven in welke situaties een beveiligingsplan vereist is.

Artikel 4.2 (aanwijzing gevallen waarin een beveiligingsplan is vereist)

De verplichting tot het zorgen voor een beveiligingsplan krachtens artikel 4.7, eerste lid, van het besluit, berust op de ondernemer die houder is van een vergunning voor het verrichten van handelingen met categorie 1-, 2-, of 3-stoffen.

In bijlage 4.1 is de categorie-indeling van de radioactieve stoffen opgenomen. Deze is verder uitgewerkt in bijlage B van deze handreiking.

Note: In deze bijlage is de indeling onjuist weergegeven. Er staat A/D>1000 dit moet zijn A/D ≥ 1.000; Er staat 1000 >A/D >10 dit moet zijn 1.000 > A/D ≥ 10.

Dit rapport is een uitgave van de

Autoriteit Nucleaire Veiligheid en Stralingsbescherming
ANVS
Koningskade 4 | 2596 AA Den Haag
Postbus 16001 | 2500 BA Den Haag

www.anvs.nl

April 2021