FANC

FEDERAAL AGENTSCHAP VOOR
NUCLEAIRE CONTROLE

AFTERCARE

Intern en extern personeel

April 2024

FANC AFCN

FEDERAAL AGENTSCHAP VOOR NUCLEAIRE CONTROLE

AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

Aftercare voor intern en extern personeel

Contents

1. Introductie

Dit document is de conclusie van het project 'Aftercare voor intern en extern personeel', in het kader van 'insider threat'. De nucleaire exploitanten en vervoerbedrijven die werken in de nucleaire en radiologische sector, moeten rekening houden met de 'insider threat' en een programma uitwerken tegen deze dreiging.

Het doel van dit project was het uitvaardigen van richtlijnen voor de uitwerking van preventieve maatregelen tegen een 'insider adversary'.

In de nucleaire sector bestaat momenteel een duidelijke regelgeving over screenings (veiligheidsmachtigingen/veiligheidsattesten/toegangsvergunningen). Een persoon die toegang heeft tot de gevoelige zones of informatie van de nucleaire installaties of vervoerbedrijven, zal een screeningsproces hebben doorlopen. Een screening is echter maar een momentopname, een foto van de situatie van een persoon op een bepaald moment in de tijd, waarbij naar het verleden wordt gekeken om een inschatting te maken van iemands gedrag in de toekomst. Daarom is het belangrijk om, naast de screening, te beschikken over maatregelen die de betrouwbaarheid van een persoon kunnen opvolgen. De persoon kan dus opgevolgd worden via een 'trustworthiness programma'.

Hierbij zal voornamelijk worden gekeken naar de 'life cycle' van de werknemer. Het doel is om een overzicht te geven van de mogelijke acties die de nucleaire installaties of vervoerbedrijven kunnen nemen, alsook een overzicht te kunnen geven van waar de grens ligt met wat op dit ogenblik wettelijk kan en wat niet kan in het kader van het nakijken/opvolgen van iemands betrouwbaarheid. Het is aan de nucleaire installaties of vervoerbedrijven om de maatregelen die zij nuttig achten, binnen hun bedrijf in praktijk te brengen en te beslissen op wie deze maatregelen van toepassing zullen zijn. De verantwoordelijkheid voor de implementatie van de maatregelen ligt bij de sector. Het FANC wijst ook op het nodige overleg dat voorafgaandelijk met eventuele sociale partners dient te gebeuren en eventuele aanpassingen in het arbeidsreglement.

In de eerste meeting van maart 2021 werd er voornamelijk gefocust op de doelstelling van dit project, alsook op enkele basisprincipes die in acht dienen genomen te worden.

In de tweede meeting van februari 2022 werd er verder ingegaan op de basisprincipes van een goede 'Security Culture'.

In de derde meeting van december 2022 werd een overzicht gegeven van concrete maatregelen die extra kunnen genomen worden tijdens de 'employee life cycle'.

In de vierde meeting van juni 2023 werd gekeken naar de acties die kunnen genomen worden ter opvolging van personeel terwijl zij werkzaam zijn in de organisatie en naar de verschillende partners die informatie zouden kunnen bezitten.

In het vijfde deel in november 2023 werd gekeken naar hoe deze informatie kan opgevolgd en verder behandeld worden.

En in de laatste meeting van maart 2024 werd dit alles geconsolideerd in één document en werd er nog gefocust op de continue verbetering.

Het gaat hier om een ondersteunende leidraad. Het blijft echter steeds de verantwoordelijkheid en de keuze van de organisatie zelf welke maatregelen er worden geïmplementeerd en hoe.

2. Wat is insider threat, waarom een dreiging?

De dreiging van eigen personeelsleden (insiders) die intentioneel een (poging tot) ongeoorloofde actie verrichten, gericht op of door gebruik van nucleair of ander radioactief materiaal, of geassocieerde instellingen, transportfirma's of activiteiten, is zeker aanwezig.

Voor de definiëring van de "insider threat" kijken we naar de IAEA Nuclear Security Series No.8-G (Rev1). Een insider wordt aanzien als: *"Een individu met geautoriseerde toegang tot nucleair materiaal, nucleaire installaties of activiteiten of tot gevoelige informatie of gevoelige informatiebronnen, die een criminele of ongeautoriseerde actie intentioneel verricht of faciliteert, tegen nucleair materiaal, ander radioactief materiaal of geassocieerde activiteiten"*.

Meer bepaald heeft een insider de '**toegang**', de '**autoriteit**' en de '**kennis**' en deze persoon kan een dreiging vormen van zodra hij/zij de intentie heeft om een ongeautoriseerde actie te verrichten of te faciliteren.

Om zich te kunnen beschermen tegen de 'insider threat' moet een combinatie van preventieve en beschermende maatregelen genomen worden binnen een organisatie:

- Preventieve maatregelen (vóór een actie): om het aantal mogelijke 'insider threats' te minimaliseren en om de mogelijkheid van een ongeautoriseerde actie door een insider te reduceren;
- Beschermende maatregelen (na een actie): maatregelen om na een insider-actie de situatie op te lossen en de ernst van de actie te mitigeren.

Idealiter zouden de preventieve maatregelen voldoende moeten zijn om alle pogingen tot potentiële insider-acties te verhinderen, maar helaas bestaat er geen mogelijkheid om een volledig overzicht te krijgen van gedragsindicatoren die een insider-actie voorspellen. We kijken hierbij nog steeds naar menselijk gedrag, wat moeilijk te voorspellen is. Uit studies is echter gebleken dat er bij insider-acties vaak wel indicatoren zijn die op voorhand zichtbaar zijn. Het zijn deze indicatoren waarop moet worden gewerkt om preventie mogelijk te maken. Al is het ook nodig om beschermende maatregelen te nemen, voor deze gevallen waarin preventie niet mogelijk was.

De insider-dreiging werd opgenomen in de Design Basis Threat-analyse. Wat de concrete dreiging is, wordt dan ook daar verder beschreven. De motivatie van een insider kan echter sterk variëren, enkele voorbeelden: geld, ideologie, wraak, ego, bedreiging of een combinatie hiervan. Dit is dus ook sterk individueel. De moeilijkheid daarbij is om op te merken dat een persoon een bepaalde motivatie begint te ontwikkelen of ontwikkeld heeft, om dus de dreiging effectief te identificeren en er actie tegen te kunnen ondernemen.

3. Trustworthiness-programma

A. Algemeen

In een trustworthiness-programma worden de ongewenste of verdachte gedragingen of karakteristieken bestudeerd om te bepalen of iemand een dreiging zou kunnen zijn. Bij een trustworthiness-programma moeten er garanties kunnen worden geboden dat de personen die worden opgevolgd, betrouwbaar zijn tot op het niveau dat zij geen onredelijk risico vormen voor de gezondheid, veiligheid en beveiliging van de organisatie en de andere personeelsleden.

Dit is heel moeilijk, want de intentie van een insider kan onmerkbaar zijn en de gedragspatronen van iemand die een dreiging vormt, kunnen significant verschillend zijn of een andere oorzaak hebben. Onderzoek heeft echter wel aangetoond dat een aantal gedragingen of karakteristieken een indicator kunnen zijn voor een grotere kans dat een individu een intentionele niet-geautoriseerde actie zal ondernemen. Dit zijn interne, externe en contextuele factoren die de persoon in de richting duwen van een ongeautoriseerde, bewuste actie om een reactie uit te lokken.

Enkele van deze gedragingen (niet-limitatieve lijst) zijn:

- 'Anger management' problemen
- Associatie met of sympathieën voor criminele of terroristische groeperingen
- Moeilijkheden om feedback of kritiek te accepteren
- Confronterend gedrag
- Ontevredenheid op het werk
- Niet accepteren van gezag
- Drugs- of alcoholmisbruik
- Sociaal isolement
- Financiële problemen
- Onwil om regels en procedures te volgen
- …

Een trustworthiness-programma heeft verschillende onderdelen. Het gaat om een proces om informatie te verzamelen over specifieke personen, om de informatie te analyseren aan de hand van gespecifieerde criteria en om te bepalen of de betrouwbaarheid van een persoon voldoende verzekerd kan worden. Het gedrag en de betrouwbaarheid van een persoon kan echter doorheen de tijd ook veranderen. Daarom is het noodzakelijk om in het programma ook voldoende trustworthiness-beoordelingen te maken tijdens de loopbaan van de persoon.

Het gaat hierbij om de opvolging van personen naast de wettelijke screenings die voorzien zijn in de wetgeving. Gedrag kan immers doorheen de tijd veranderen. Er wordt hierbij een rol weggelegd voor de Veiligheidsofficier om het gedrag op te volgen van personen die een screening ondergingen (art. 13/1, par. 1, b. Wet van 11 december 1998 [betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen). Een Veiligheidsofficier kan dit echter niet alleen opvolgen voor het volledige personeel. Mechanismen moeten worden ingevoerd om informatie tot bij hem/haar te laten komen en er moet binnen de organisatie een kader worden gemaakt om informatie op te volgen. Dit zal moeten worden gedefinieerd in procedures, alsook de functie van de personen die deel uitmaken van de groep die de informatie zal behandelen (vb. HR). Gaat het om personen in een pre-employment screening of mensen die geen wettelijke screening dienen te ondergaan, dan is er een rol weggelegd voor de HR-dienst.

B. Basisprincipes

Overzicht :

1. Het management heeft een voorbeeldfunctie en de principes moeten dus ook worden gedragen binnen het management.
2. Een gedragen Security Culture binnen de organisatie is de basis: het personeel moet beveiliging mee als hun verantwoordelijkheid zien en daarbij de signalen van verandering van gedrag van personen opmerken en eventueel doorgeven.
3. Het personeel moet niet worden aanzien als een permanente dreiging, maar als een eventueel middel om met een dreiging om te gaan.
4. De basis van een 'Trustworthiness-programma' is een goed personeelsbeleid: om ervoor te zorgen dat werknemers zich niet tegen de organisatie keren, moeten zij tevreden zijn binnen hun werkomgeving.
5. Mensen moeten worden ingezet op de goede plaats: niet enkel op vlak van technische capaciteiten, maar ook de persoonlijkheidskenmerken moeten in acht worden genomen (vb. stressbestendigheid, …).
6. Er moet worden gewerkt met een 'graded approach': niet alle middelen inzetten op iedereen, maar afhankelijk van de toegang, gezag, hiërarchische positie en kennis moet een analyse worden gemaakt welke functies de meeste schade kunnen aanrichten.
7. Er moet een duidelijk overzicht worden gegeven, vb.: wat zijn gedragingen die kunnen worden opgepikt, deze gedragingen duidelijk definiëren (om ook achterdocht te vermijden), criteria voor determineren van iemands betrouwbaarheid, maar ook mogelijke reacties moeten worden gedefinieerd en wie welke beslissing neemt (bijkomend onderzoek bij de NVO, eventuele klacht bij politie, tijdelijke verandering van functie, ontslag, …) en hoe men snel actie kan nemen (in sommige gevallen is een directe actie zeker noodzakelijk).
8. Privacyregels: er dient rekening te worden gehouden met de privacyregels die van toepassing zijn in België. Het trustworthiness-programma moet in evenwicht zijn met de rechten van de persoon. Een goede beschrijving van het programma en de mogelijke maatregelen zijn hiervoor alvast een goed begin.

4. Security Culture

A. Algemeen

Een integrale 'Security Culture' is een belangrijk element in het kader van Aftercare. Dit zou in de algemene bedrijfscultuur moeten worden opgenomen, zodat dit voor iedereen een gewoonte wordt, zoals dit momenteel ook het geval is met de veiligheidscultuur.

Als we kijken naar de definities van een 'cultuur', kunnen we concluderen dat het gaat om de ideeën, de gewoontes en de waarden van een specifieke groep. Dit houdt in dat beveiligingsregels en -principes algemeen moeten gekend zijn en worden gebruikt, zodat het voor de mensen een tweede natuur wordt om hierop te reageren. Het algemene doel hierbij is dat zowel het interne als het externe personeel vrijwillig en bewust beveiliging als hun verantwoordelijkheid ziet.

De moraal van het personeel en hun loyaliteit ten opzichte van de organisatie (nucleaire exploitant of vervoersbedrijf) zijn belangrijke aspecten in het kader van de interne dreiging of

'insider threat'. Men kan er namelijk vanuit gaan dat mensen die loyaal zijn ten opzichte van hun organisatie en binnen deze organisatie een goede moraal hebben, minder een dreiging vormen ten opzichte van deze organisatie, gezien zij minder geneigd gaan zijn om een actie te ondernemen om deze organisatie te schaden. Een 'no blame'-cultuur om zaken bespreekbaar te maken, kan hierbij ondersteunen.

Het is belangrijk dat iedereen binnen het bedrijf zich bewust is van de beveiligingsmaatregelen en -procedures en dat men op de hoogte is van het bestaan van de interne dreiging, alsook van de mogelijke consequenties. Het goed beheersen van de verschillende procedures en hoe men op situaties dient te reageren is dan ook een van de maatregelen tegen de 'unwitting insider' (misbruik van iemands toegang, zonder dat de persoon zich ervan bewust is). Opleiding en training over deze procedures en regels zijn dan ook noodzakelijk.

De opleidingen rond de interne dreiging moeten daarentegen ook wel met de nodige nuance naar voor kunnen worden gebracht. Iedereen moet zich bewust zijn van de dreiging en de mogelijke consequenties, maar het is niet de bedoeling om iedereen te wantrouwen en hierbij iedereen als een dreiging te zien. Binnen deze dreiging is het echter belangrijk om zich bewust te zijn van het gedrag van het personeel en dat aanpassingen van dit gedrag of verdacht gedrag naar boven worden gebracht zodat dit kan worden opgevolgd. Een verandering in het gedrag is echter niet standaard een bewijs van een mogelijke interne dreiging. De persoon kan ook met andere problemen of uitdagingen te kampen hebben, waardoor een melding/rapportering van dergelijk gedrag ook kan leiden tot de nodige hulp en ondersteuning van de persoon. Dit dient als één geheel te worden aanzien. Door rapportering kan men de persoon de nodige ondersteuning proberen bieden, of hij/zij nu effectief een interne dreiging begon te vormen of niet. Rapportering zou een tweede natuur moeten worden en maximaal zonder noodzaak tot opleggen van sancties, dit ook om zelfrapportering mogelijk te maken (zonder dat het een vrijgeleide is om regels te breken).

Het is daarom ook belangrijk dat er zo vroeg mogelijk kan worden ingegrepen wanneer wordt opgemerkt dat iemand eventueel in de richting van een interne dreiging zou neigen. Zolang er niet effectief een actie is ondernomen, kan immers alles nog worden verhinderd en kan de persoon zijn gedrag nog aanpassen. Hierbij is het belangrijk dat de directe collega's in de mogelijkheid zijn om dergelijke aanpassingen in gedrag of wangedrag onderling bespreekbaar te maken en te rapporteren. Dit maakt deel uit van de 'Security Culture'. Men dient ook op de hoogte te zijn van de opvolging van rapporteringen, zodat men ook weet dat de informatie goed zal worden opgevolgd en bekeken, dit om te verhinderen dat personen niets durven rapporteren uit angst voor sancties.

B. Interface met 'IAEA Nuclear Security Series No. 7 Nuclear Security Culture: implementing guide'

Als we kijken naar de richtlijnen van het IAEA rond 'Security Culture', komen we tot onderstaand schema:

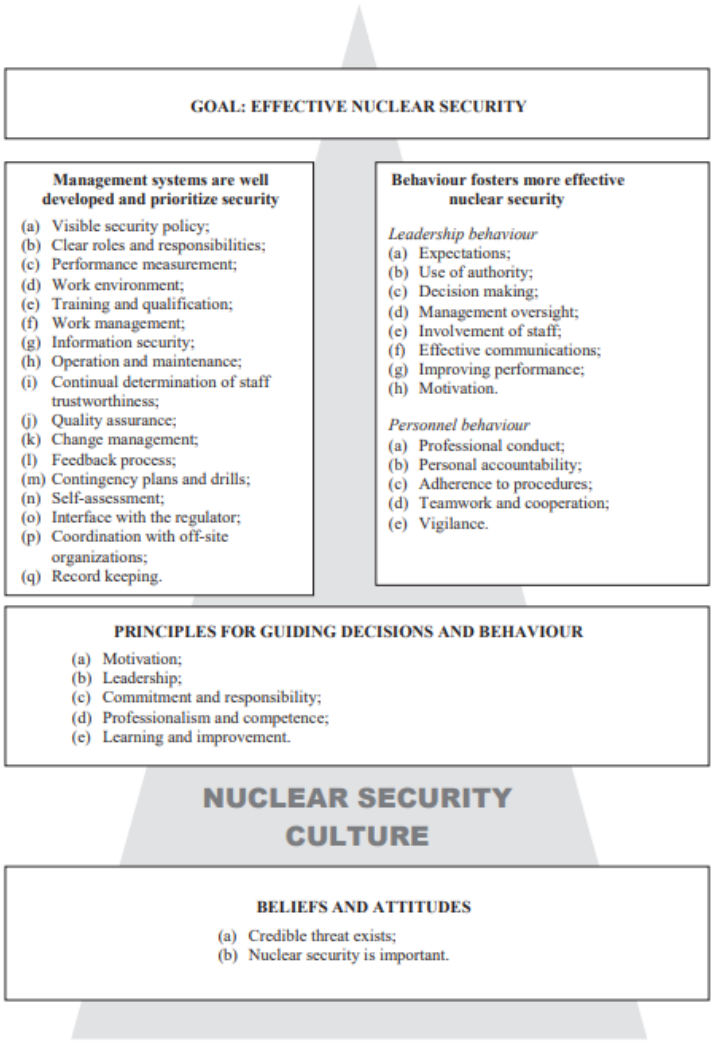

FIG. 2. Characteristics of nuclear security culture.

Het is duidelijk dat enkele aspecten een directe impact hebben op de notie 'Aftercare', we denken voornamelijk aan:

- Duidelijke rollen en verantwoordelijkheden: de rol van iedereen binnen de organisatie dient te worden geduid, alsook de rol van het opvolgen van gerapporteerde informatie;
- Werkomgeving: wanneer iemand in een goede werkomgeving functioneert en zich loyaal voelt ten opzichte van een organisatie, zal die persoon minder snel een dreiging vormen tegen de organisatie;

- Training: er moet voldoende awareness en opleiding over de interne dreiging en 'aftercare' worden voorzien;
- Continue opvolging van trustworthiness: iedereen binnen een organisatie dient elkaar mee op te volgen. Bij twijfel of veranderingen dient gedrag te worden gerapporteerd voor verder onderzoek;
- Leiderschapsgedrag: het management dient het voorbeeld te geven om de beveiligingscultuur draagkracht te geven (meer hierover in punt C);
- Gedrag van personeel: de organisatie wordt gedragen door het personeel. Het is dus belangrijk dat iedereen weet welk gedrag van hen wordt verwacht en dat zij de beveiliging van de organisatie mee als hun verantwoordelijkheid zien, om ervoor te zorgen dat de procedures worden gevolgd. Er moet een duidelijke grens worden gevonden tussen aanvaardbaar en onaanvaardbaar gedrag;
- Overtuigingen en gedrag: dit blijft de basis van de hele beveiligingscultuur.

De beveiligingscultuur dient dus in de organisatie ingebed te zijn en ieders rol en verantwoordelijkheid dienen hierin te worden opgenomen. Belangrijk is ook dat dit niet een onderwerp is dat enkel door het beveiligingsdepartement moet worden gedragen, maar dit dient in de eerste plaats door het management in de organisatie te worden getoond. Zij dienen er dan ook voor te zorgen dat er voldoende middelen (personeel en financieel) en ruimte is om deze cultuur aan te moedigen. Er moeten voldoende procedures en structuren worden opgezet, maar er dient ook een focus te zijn om regelmatige opleidingen en opvolging van gerapporteerde informatie mogelijk te maken.

De 'Security Culture' dient ook regelmatig te worden geëvalueerd om het mogelijk te maken om steeds te verbeteren. Ook hierover zijn er richtlijnen van het IAEA over de 'self-assessment' van de beveiligingscultuur (NSS No. 28-T), die deze evaluatie kunnen ondersteunen.

C. Rol van het management binnen Security Culture

De beveiligingscultuur dient door iedereen te worden gedragen. De informatie moet bottom-up naar boven komen en ook dient er in de gehele organisatie te worden aangegeven wanneer bepaalde maatregelen niet werkzaam zijn, zodat dit kan worden herbekeken. Het is echter belangrijk om hier ook een 'top-down'-benadering voor op te nemen, anders zal dit niet slagen. Het is dus niet enkel de verantwoordelijkheid van het beveiligingsdepartement, maar ook senior management en elke ander departement dienen hierin hun rol te spelen.

Management dient zelf ook beveiliging in acht te nemen en zijn gedrag hierop af te stemmen, zodat iedereen binnen de organisatie dit met de nodige verantwoordelijkheid zal opnemen. Hierbij is het nodig dat, gezien hun hiërarchische positie, zij zelf ook een overzicht dienen te bewaren van de betrouwbaarheid van het personeel in de organisatie, zowel internen als externen.

Een managementsysteem met duidelijke verantwoordelijkheden, rollen en procedures kan hierin enorm ondersteunen en is noodzakelijk. Hierdoor heeft men een richtlijn van gedragingen en verwachtingen, waardoor het efficiënter zal zijn om de continue opvolging van de betrouwbaarheid van personeel te waarborgen. Dit kan heel concreet ook een duidelijker beeld geven van de gedragingen en karakteristieken waarnaar moet worden uitgekeken (zie

bijlage A), zoals bijvoorbeeld: professioneel gedrag, persoonlijke aansprakelijkheid, volgen van procedures, teamwerk, samenwerking, voorzichtigheid, …

D. Concrete maatregelen die kunnen worden genomen

Hieronder een overzicht van maatregelen die in het kader van Security Culture kunnen worden genomen om dit onderwerp te ondersteunen:

- Opleidingen + trainingssessies: bij binnenkomen in organisatie, met nodige herhalingen. Dit dient ook te worden voorzien voor extern personeel:
  - Wat is insider threat?
  - Mogelijke motivatie
  - Rol van iedereen hierin – verantwoordelijkheid van iedereen
  - Ondersteunen van collega's en reageren bij mogelijke problemen van collega's
  - Maatregelen die hiervoor worden genomen: beperken van toegang, spreiding van taken, two-person rule, …
  - Mogelijke impact
  - Door vroege identificatie: hulp kan worden geboden aan de persoon, geen consequenties voor persoon en voor omgeving
- Awareness campagnes
  - Badge dragen
  - Cyberaspecten → up-to-date houden
  - Rapporteringen
  - …
- Externen:
  - Onderlinge samenwerking tussen de veiligheidsofficieren
  - Opnemen in contracten dat hier aandacht aan moet worden besteed
  - Opnemen van opleiding
- Algemeen HR-beleid: focus op moraal van personeel en goed beleid
  - Goede mensen op goede plaats, niet enkel naar kennis kijken, maar ook naar persoonlijkheidskenmerken ten opzichte van de functie
  - Goede werkomgeving
- Evaluatie beveiligingscultuur: periodieke evaluatie van de verschillende aspecten van de beveiligingscultuur

5. 'Trustworthiness'-opvolging van het personeel

A. Algemeen

Maatregelen worden best genomen in een 'graded approach'. Dit houdt in dat er een analyse dient te gebeuren van wie toegang heeft tot wat (materiaal, documenten en zones) en de kennis die de persoon in het kader van zijn/haar functie bezit (risicoprofiel opstellen). Op basis hiervan kan men bepalen welke personen meer dienen te worden opgevolgd dan anderen.

Deze analyse kan gebeuren op basis van de functies en de specifieke toegangen gelinkt aan deze functies. In een tweede lijn kan men eventueel wel de maatregelen verhogen of uitbreiden als iemand reeds meerdere functies heeft bekleed en dus een hoger niveau van kennis heeft

waardoor extra aandacht moet worden besteed. Het doel is om de maatregelen te linken aan het risico en de impact van de consequenties van een bewuste insider-handeling.

Het doel van een 'trustworthiness'-programma is te bepalen of iemand betrouwbaar is, de opvolging van het personeel om veranderingen in gedrag op te merken, maar het kan ook een afschrikkende werking hebben (wanneer men weet dat verandering van gedrag zal worden opgemerkt). De bepaling van iemands 'trustworthiness' gebeurt best voor aanwerving, tijdens de werkzaamheden en op het einde van de werkzaamheden. Het gaat hier om een combinatie van verschillende maatregelen afhankelijk van de situatie. In de nucleaire sector is al een overheidsscreening voorzien. In dit document gaan we oplijsten welke de mogelijke extra maatregelen zijn die kunnen worden genomen. Er dient verder per organisatie te worden bekeken welke maatregelen we kunnen ondersteunen en kunnen worden geïmplementeerd (en op welke manier).

B. Privacy

Deze bijkomende maatregelen, naast de reeds bestaande wettelijke screenings, kunnen alleen worden uitgevoerd voor een specifiek, uitdrukkelijk doel, in dit geval de beveiliging tegen interne dreiging. De werkgever heeft een legitiem belang om bepaalde controles uit te voeren. Hierbij dient hij evenwel de werknemers of de kandidaat (in het kader van pre-employment) voldoende in te lichten over alle aspecten van deze bijkomende maatregelen (de doeleinden, bewaartermijnen, mogelijke acties, …). Het documenteren van deze processen (zie deel C) is reeds belangrijk tijdens een sollicitatie en dient steeds te worden gecommuniceerd.

Per maatregel is het belangrijk om aan te geven wat het doel is en dus om een overzicht te hebben van de gegevens die men verwerkt. Zodra de werknemer niet meer tewerkgesteld is in de organisatie, dient men de gegevensverwerking te stoppen.

Er dient bij deze maatregelen steeds rekening te worden gehouden met het proportionaliteitsbeginsel en, zoals reeds meermaals werd vermeld, volgen we de principes van een graded approach.

Er dient tijdens dit proces over gewaakt te worden dat men niet aan profilering[1] zal doen, tenzij men het kan verantwoorden binnen de uitzonderingen voorzien in de privacywetgeving. Bij de analyse zal altijd nog menselijke tussenkomst nodig zijn.

Het is belangrijk om in dit proces te voldoen aan de nodige vereisten van de privacywetgeving.

C. Documenteren

Het is belangrijk om aan te geven wie verantwoordelijk is voor het 'trustworthiness'-programma. Binnen de wetgeving van toepassing op de nucleaire sector is het de taak van de veiligheidsofficier om de personen in het bezit van een veiligheidsmachtiging/veiligheidsattest op te volgen. De veiligheidsofficier dient hiervoor echter te worden ondersteund door de organisatie, anders kan dit niet op een efficiënte manier gebeuren. De veiligheidsofficier kan

[1] Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

hiervoor een samenwerking voorzien met departement beveiliging, HR, directe lijn met line management en eventuele andere personen binnen de organisatie met een relevante input.

Het is belangrijk dat alle processen, verantwoordelijkheden, acties en rapporten goed gedocumenteerd zijn. Door zo open mogelijk te zijn over de verschillende processen en werkzaamheden, zal het programma meer vertrouwen kunnen krijgen. Er dient bij dergelijke samenwerking op voorhand te worden bepaald wie toegang heeft tot welke informatie en waar het wordt opgeslagen, zodat iedereen hiervan op de hoogte is.

Het personeel dient dan ook voldoende te worden opgeleid en alle nodige informatie te verkrijgen om verdere acties te kunnen nemen, indien nodig.

Dergelijk programma wordt best regelmatig geëvalueerd, om uitdagingen en moeilijkheden te identificeren en alles zo efficiënt mogelijk te laten verlopen.

De maatregelen die in dit document worden beschreven, gaan over het verzamelen van informatie. Vervolgens zullen we in het project verder gaan met suggesties rond rapportering, het analyseren van de data en eventuele acties.

Belangrijk is daarbij dat alle bijkomende maatregelen gelijk zijn voor iedereen. Hiermee bedoelen we: gelinkt aan bepaalde functies (graded approach). De maatregelen die worden gekozen, dienen voldoende te worden beschreven in het arbeidsreglement, -contract en de privacyverklaring. Het is echter aan de nucleaire exploitant of het vervoerbedrijf om te bepalen welke maatregelen kunnen ondersteunen in hun 'trustworthiness'-programma en dus binnen hun organisatie kunnen worden uitgewerkt.

D. Concrete maatregelen die kunnen worden genomen

Pre-employment acties:

- Achtergrondcheck:
    - Identiteit verifiëren: eventueel ook via specifieke systemen voor de verificatie van de identiteitskaart;
    - Werkhistoriek nakijken van de werknemer[2]: vragen om een document in te vullen met vorige werkgevers en contactgegevens, en toestemming vragen om de gegevens na te kijken;
    - Open-source verificatie/sociale media: de gegevens mogen worden bekeken, maar let op met verdere verwerking hiervan;

[2] Standpunt van de GBA: De kandidaat geeft zijn toestemming door een verklaring te ondertekenen waarvan hij de draagwijdte duidelijk kan begrijpen en die ten minste de volgende verklaringen bevat:

1. zijn identiteit en de identiteit van de organisaties of de personen die de werkgever wil raadplegen;
2. de aard van de gevraagde gegevens;
3. de redenen voor het verzamelen van de gegevens;
4. de periode waarin de toestemming zal worden gebruikt.

Als een referentiepersoon in het cv wordt vermeld, kan dit gelden als een toestemming van de kandidaat. In ieder geval mag de werkgever de informatie die de kandidaat aan hem heeft doorgegeven niet systematisch bij derden controleren. Als een cv duidelijk hiaten vertoont, moet de werkgever de kandidaat eerst zelf vragen naar deze duidelijke 'lacunes' in zijn opleidings- en loopbaantraject. Pas als de uitleg van de kandidaat over het onderwerp niet afdoende was, kan de potentiële werkgever overwegen gegevens van andere personen of organisaties te verzamelen, op voorwaarde dat de kandidaat daarvan vooraf op de hoogte is gesteld en daarvoor zijn toestemming heeft gegeven.

  - Opvragen strafregister: het basisdocument kan worden opgevraagd en bekeken, verdere verwerking ervan kan niet;
  - Financiële check: een uittreksel van de bestanden CKP (Centrale voor Kredieten aan Particulieren) en ENR (niet-gereglementeerde registraties) kan worden opgevraagd. Dit is echter bijkomende informatie, want dit kan niet specifiek worden gebruikt om iemand te weren. Het vermogen van een persoon is beschermd onder de discriminatiewetgeving van 10 mei 2007[3].

  ➔ Voorbeeld uit de sector: enkel een checklist van de consultatie van de informatie hierboven wordt bewaard, de documenten met de persoonsgegevens zelf worden vernietigd.
- Onderzoek door een privédetective: zeker te determineren op voorhand voor welke functies en welke info relevant is;
- In acht nemen van de competenties en gedragingen van de persoon, om zeker te zijn dat deze in lijn zijn met de job, eventueel via een personal assessment of een diepgaand interview gefocust op de gezochte competenties;
- Gedocumenteerd screeningsproces (ook als deel awareness op voorhand): toelating vragen voor een Trustworthiness check en aangeven dat er onderzoeken zullen worden gedaan en dat er een continue opvolging zal zijn van de gedragingen van de persoon (aangeraden is om dit deel te laten uitmaken van het arbeidscontract);
- Positieve screening (veiligheidsattest/toegangsvergunning/veiligheidsmachtiging) is een vereiste voor het contract;
- Training van diegenen die rekruteren op vlak van insider threat en het herkennen van signalen rond verdachte gedragingen;
- Documenteren van het rekruteringsproces om de transparantie te verhogen;
- Documenteren van de beslissingen in een rekruteringsproces;
- Rekruteringsjury samengesteld uit verschillende actoren uit de organisatie;
- Duidelijke, coherente lijst van veroordelingen en gedragingen (indien mogelijk) die niet worden geaccepteerd in functie van de verantwoordelijkheden.

→ Voorbeeld uit de sector: een aparte dienst (of privédetective) die bepaalde informatie bekijkt/opvraagt om een beveiligingsadvies op te stellen. Dit kleurt de visie van HR niet en er is een advies waarmee verder kan worden gewerkt binnen het aanwervingsproces. Het strafregister bijvoorbeeld kan dan apart worden behandeld en niet verder worden verwerkt.

Employment:

- Transparantie:
  - Bezit van een duidelijke 'code of conduct': ook een kort, duidelijk overzicht toegankelijk maken, niet enkel een hele reeks regels;
  - Overzicht van alle maatregelen die worden genomen in het kader van insider threat: transparantie verhogen;
  - Duidelijk gekend systeem van rapportering: over uzelf en over anderen;

[3] 10 MEI 2007 - Wet ter bestrijding van bepaalde vormen van discriminatie

    - Duidelijke procedures over de acties die worden genomen en de onderzoeken die starten bij het bekomen van informatie = administratief onderzoek + de rechten die de persoon zelf kan laten gelden;
- Verschillende rapporteringsmechanismen nodig;
- Open en ondersteunende cultuur creëren ("no blame culture");
- Systeem van permanente mentoring/coaching/buddy om een directe, continue opvolging te voorzien in het kader van opleiding, maar ook in het kader van opvolging;
- Jaarlijkse verplichte security briefings: basis rond veiligheidsmachtigingen en hoe om te gaan met informatie, mogelijke gevolgen bij niet omzichtig omspringen, aspect Security Culture, dreiging van Insider;
- Training voor werknemers en management om 'red flags' te identificeren, een cultuur van signalisatie als gevolg van opleidingen voor het detecteren en signaleren van alarmsignalen in hun context en het definiëren van de middelen om te signaleren, onder meer door het gebruik van POC (Person of Contact) → doel: kenbaar maken aan de werknemers dat ze hun collega's kunnen ondersteunen en hun bezorgdheden naar boven kunnen laten komen;
- Creatie van een insider threat mitigation team: management, beveiliging (veiligheidsofficier), ICT, HR, juridische dienst;
- Concreet opvolgingssysteem om systematisch wijzigingen door te geven, intern en aan de NVO: adreswijzigingen, wijzigingen in gezinssituaties, buitenlandse reizen;
- Terugkerende vaste meetings met elk personeelslid en hierbij telkens een analyse opstellen rond zijn trustworthiness op basis van:
    - Checklist
    - Standaard vragenlijst op basis van objectieve criteria
- Opvolging van het digitaal gedrag van personen (toegang tot zones, documenten, surfgedrag, …);
- Systematisch opvragen van strafregister om de X jaar: het basisdocument kan worden opgevraagd en bekeken, verdere verwerking ervan kan niet (te voorzien in het arbeidsreglement + verantwoording nodig);
- Meetings mogelijk maken op basis van verkregen info: gerapporteerde info (zelf gerapporteerd of via iemand anders);
- Terugkerende meeting met een geïdentificeerd team om eventueel personen/incidenten te bespreken: gebaseerd op algemene statistieken en de vraag of er terugkomende meldingen zijn van bepaalde personen. Hierbij ook de algemene informatie die in het bezit is van HR (aandacht houden voor een 'conflict of interest');
- Een beroepsproces in het geval van een onenigheid met management;
- Duidelijkheid omtrent mogelijkheid om naar vertrouwenspersonen te gaan;
- Duidelijkheid rond mogelijkheden voor psychosociale analyses;
- Systemen om de signalen van vertrouwenspersonen en bijkomende analyses op te vangen;
- Beperken van toegang van werknemers gebaseerd op specifieke redenen die moeten worden gedocumenteerd;
- Auditering van systemen en toegang;
- 4-eyes-principle;
- Alarmsystemen op toegangssystemen;

- Secure toegang tot digitale systemen die worden gelogd;
- Verdeling van specifieke rollen en verantwoordelijkheden;
- In specifieke gevallen: men kan in gedocumenteerde situaties werken met een privédetective.

Maatregelen in geval van twijfel of langdurige afwezigheid:

- Toegang beperken (op algemene basis die moet worden gedocumenteerd)
- Bijkomende informatie doorgeven aan de NVO met vraag voor bijkomend onderzoek
- Bijkomende maatregelen (bijkomende trustworthiness meeting, ...)

Post-employment/upon termination:

- Een duidelijk 'off-boarding' plan;
- Documenteren van een ontslagproces;
- Toegang ontzeggen, zowel fysiek als digitaal (hierbij dient ook een onderscheid in procedure te worden gemaakt tussen een gedwongen en vrijwillige beëindiging van het arbeidscontract);
- Teruggave van alle arbeidsmiddelen van de organisatie (badges, IT-apparatuur, ...);
- Confidentialiteitsclausule/-contract.

6. Human Reliability Programme

A. Personeelsbeleid

Werknemers dienen in hun werkzaamheden te worden ondersteund. Dit houdt in dat er een personeelsbeleid moet worden gevoerd waarin mensen worden gehoord en er naar hen wordt geluisterd. Dit ondersteunt de vorming van solide menselijke relaties, georiënteerd op het personeel.

Hiervoor dienen de nodige middelen te worden ingezet om de verzuchtingen van het personeel op te vangen en hier vervolgens in de mate van het mogelijke acties rond te nemen. Iedereen binnen de organisatie moet in staat zijn om bemerkingen over de manier van werken, medewerkers en hiërarchische lijn door te geven. Hier zijn ook de nodige modaliteiten voor binnen de wetgeving rond personeelsbeleid.

Deze mogelijkheden om te worden gehoord, dienen voldoende kenbaar te worden gemaakt; dit om ervoor te zorgen dat het toegankelijk en laagdrempelig is om bepaalde zaken kenbaar te maken, wat bijdraagt tot de gangbaarheid van dergelijke meldingen. Dit zal ook ondersteunen in mogelijkheden rond rapportering.

Medewerkers dienen zich goed te voelen in hun organisatie om het risico te verlagen dat ze iets ondernemen om de organisatie te schaden. Dit start bij een goed personeelsbeleid en een ondersteunende cultuur. In het kader van de maatregelen tegen 'insider threat' helpt het om medewerkers op de juiste plaats in te zetten, niet enkel met de juiste kennis, maar ook in een omgeving die voor hen werkt.

B. Informatievergaring ter opvolging van veranderend gedrag

Periodieke evaluaties

Periodieke evaluaties van alle werknemers is een methode om op regelmatige basis te peilen naar het welzijn van een persoon, hoe hij/zij zich op het werk voelt en hoe hij/zij het werk

uitvoert. Dit geeft de mogelijkheid aan een N+1 om een regelmatig en hopelijk goed contact te hebben met de werknemers en bepaalde acties of gedragingen uit te klaren, indien nodig. Dit geeft ook de mogelijkheid om eventuele veranderingen van gedrag te kaderen in specifieke omstandigheden. Deze zijn genotifieerd via rapportering, waardoor dit een maatregel is tegen subjectiviteit gezien regelmatig kan worden gepeild naar de omstandigheden van de persoon en er vroeg kan worden ingegrepen.

Deze evaluaties dienen te worden gedocumenteerd en het proces dient regelmatig in herinnering te worden gebracht, zodat de medewerker hiervan op de hoogte is. Dit geeft de persoon de mogelijkheid om zijn/haar eigen acties op het werk te evalueren en eventueel aan te geven indien er iets kan worden aangepast.

Door regelmatige gesprekken te voeren, kunnen veranderingen in gedrag of reacties beter naar boven komen; iets wat in de normale gang van zaken misschien minder zal opvallen gezien de focus vaak op de outcome van het werk ligt.

Periodieke evaluaties kunnen ook worden gehouden over de gegevens die de persoon zelf vrijgeeft. Bij de aanwerving wordt bijvoorbeeld soms een social media check gedaan.

Contact met de betrokkene

Naast periodieke overlegmomenten en evaluaties, zou het steeds mogelijk moeten zijn om een overleg met een persoon te hebben wanneer er twijfels zijn bij bepaalde acties of gedrag. De organisatie dient eraan te werken dat de bedrijfscultuur dit toelaat en het toe te voegen aan haar processen.

Reguliere logging

Naast informatie van de persoon zelf, is het steeds nuttig om monitoringssystemen te hebben om anomalieën te signaleren. Het gaat hierbij voornamelijk om loggings van toegangen of pogingen tot toegang. Systemen die zelf aangeven wanneer er anomalieën zijn, maken het proces uiteraard gemakkelijker.

Rapporteringen

Gegevens die binnenkomen via een rapporteringsmechanisme zijn zeker op te volgen.

HR-wijzigingen doorgeven aan de VO

De Veiligheidsofficier (VO) is verplicht om wijzigingen in de levenssituatie van een persoon door te geven aan de Nationale Veiligheidsoverheid (NVO) indien de persoon in het bezit is van een veiligheidsmachtiging. Deze wijzigingen dienen standaard reeds te worden doorgegeven aan HR voor het personeelsdossier (rekening houdend met de maximale bewaartermijn). Een systeem en processen ontwikkelen waarbij deze gegevens via HR worden doorgegeven aan de VO kunnen dit proces vergemakkelijken. Dit kan ervoor zorgen dat deze wijzigingen systematisch worden doorgegeven aan de NVO. We denken dan aan:

- Wijzigingen in burgerlijke stand
- Adreswijzigingen

Door een communicatie te voorzien tussen HR en de VO is men zeker dat de gegevens op de correcte plaats worden aangegeven. Er dient voldoende te worden afgelijnd welke gegevens worden doorgegeven.

Verificatie van informatie

Het is uiteraard belangrijk om alle vergaarde informatie te verifiëren, om te vermijden dat men in het kader van verdachte gedragingen valse beschuldigingen zou uiten. De verificatie hangt af van de informatie zelf. Een gesprek met de persoon of aftoetsen van gegevens bij andere bronnen, zijn processen die hiervoor kunnen worden ingevoerd.

Contact met andere VO's

Gezien de hoeveelheid onderaannemers is een actieve communicatie met de VO's van deze firma's ook een bron van informatie. Deze VO's hebben dezelfde verplichtingen om de werknemers op te volgen. De ervaring toont aan dat dit niet altijd even vlot verloopt. Een goede verstandhouding met de verschillende VO's en informatie-uitwisseling kunnen echter eventuele twijfels omtrent werknemers van onderaannemers ook bespreekbaar maken.

C. Intern platform

De organisatie kan gediend zijn met de creatie van een intern platform om partners samen te brengen om eventuele 'red flags' verder te bespreken. Dit platform zit best op een niveau waarbij er actie kan worden genomen indien dit de conclusie is van de gesprekken. Dit platform kan periodiek bij elkaar komen om eventuele risico's naar boven te brengen of kan in acute dossiers ad hoc samenkomen.

De partners die hier dienen te worden samengebracht, zijn onder meer deze van HR, security en welzijn op het werk. Afhankelijk van het dossier kan hier uiteraard ook een beroep worden gedaan op de N+1, de AFB of specifieke andere personen.

Dit orgaan dient dan voldoende gekend en gedocumenteerd te zijn. Het kader waarbinnen zij werken, dient rekening te houden met de geldende privacywetgeving. Het is hierbij steeds belangrijk de verschillende belangen af te wegen (voorzichtigheidsprincipe in kader van beveiliging).

Op dit platform kunnen acties en 'red flags' van specifieke personen worden besproken. Dit geeft de mogelijkheid om gegevens van verschillende diensten samen te leggen. Zoals bijvoorbeeld:

- Rapporteringsmeldingen
- Loggings van toegang (fysiek, digitaal)
- Gegevens van periodieke evaluaties
- Gegevens gekend bij HR
- …

Let wel, de gegevens die hier worden gedeeld, dienen relevant te zijn voor de vraag of een persoon een mogelijke insider-dreiging vormt of niet. Er dient duidelijk te worden bepaald op basis van welke criteria een dossier zal worden voorgedragen. De lijst met 'red flags' kan hier eventueel in ondersteunen.

Een eenduidige verslaggeving van deze analyse en conclusie is belangrijk om aan te geven dat de analyse op een correcte en objectieve manier werd gedaan. Dit kan worden toegevoegd aan het personeelsdossier van de persoon zelf.

D. Ondersteuning bieden

Een werknemer die problemen of uitdagingen heeft naast het werk, is uiteraard geen verantwoordelijkheid van de werkgever. Indien dit echter een effect kan hebben op zijn werkzaamheden of op de betrouwbaarheid van een persoon, is dit wel weer iets om aandachtig voor te zijn.

Het kan hierbij nuttig zijn om eventueel een overzicht te hebben van de hulpverlenende organisaties in de omgeving; dit in de eerste plaats enkel informatief om de werknemer te ondersteunen.

Deze organisaties kunnen in sommige gevallen eventueel meehelpen bij de interpretatie van verdachte signalen. Dit kan ook ondersteuning bieden bij de samenwerking of het contact met de betrokken persoon.

E. Bijkomend onderzoek bij de NVO

Bij sterke twijfel bestaat de mogelijkheid om een bijkomend onderzoek te vragen. Hiervoor dient door de veiligheidsofficier contact te worden opgenomen met de NVO. Gebruik maken van deze mogelijkheid is de beslissing van de VO. Daarna is het aan de NVO om te besluiten of de informatie voldoende is.

F. Duidelijke communicatie

Het belangrijkste in heel dit proces en de opvolging van de betrouwbaarheid van een persoon is de communicatie hierrond.

Aan de ene kant dienen de processen en de procedures in dit kader goed gedocumenteerd te zijn. En aan de andere kant dient dit kenbaar te worden gemaakt aan iedereen binnen de organisatie.

Wanneer er specifieke dossiers lopende zijn, dient hier voldoende over te worden gecommuniceerd naar de betrokkene of naar degene die gegevens heeft gerapporteerd. Er wordt bij deze communicatie rekening gehouden met de betrouwbaarheid van de gegevens en de privacy van de betrokken personen. Eventueel enkel een melding dat er iets mee werd gedaan is, afhankelijk van het dossier, voldoende. Dit dient echter steeds in acht te worden genomen om komende rapportering mogelijk te maken.

7. Rapporteringsmechanismen

A. Welke meldingen?

Het vooral belangrijk om zo vroeg mogelijk signalen van verandering van gedrag proberen op te vangen. Het gaat hierbij om signalen van werknemers die toegang hebben tot de nucleaire site of vervoerbedrijf (zowel vaste werknemers als werknemers werkzaam voor een permanente of tijdelijke onderaannemer). Iedereen binnen de organisatie dient hiervan op de hoogte te zijn en mee te werken aan het verzamelen en naar boven brengen van deze signalen, juist om de organisatie en de betrokkene zelf te ondersteunen. Het gaat om observatie van de situaties die niet normaal lijken. In het algemeen verloopt het proces tot het ontstaan van een interne dreiging volgens een aantal fasen die zichtbaar zijn bij externe observatie, zelfs als het gaat om verschillende momentopnames.

Manier van melden

Het kan hierbij helpen om bepaalde zaken automatisch te laten signaleren: denk bijvoorbeeld aan pogingen tot het raadplegen van documenten zonder toestemming of toegang tot specifieke zones op ongewone momenten. Het is echter belangrijk dat iedereen binnen de organisatie aandachtig is voor deze signalen en bij de minste twijfel de mogelijkheid heeft om dit gemakkelijk door te geven. Daarbij wordt aangeraden om toegankelijke systemen te hebben, en duidelijke processen over hoe wordt omgegaan met twijfels en deze ontvangen informatie. Het zou duidelijk moeten zijn dat dergelijke signalen zullen worden opgevolgd en dat de betrokkene ondersteuning zal krijgen in plaats van te worden gestraft (zie ook de klokkenluiderswetgeving[4]). Langs de andere kant dient de organisatie hier dan ook voor open te staan.

Het is daarbij aangeraden om verschillende mogelijkheden te laten om deze elementen te melden. Denk hierbij aan de mogelijkheid om gegevens anoniem door te geven. Hierbij dient rekening te worden gehouden met afdoende veiligheids- en gegevensbeschermingsniveaus van de systemen om de integriteit van de gegevens te verzekeren (indien nodig, ook rekening houdend met de wetgeving omtrent classificatie en categorisatie). Enkele mogelijke opties:

- Online formulier;
- Vast mailadres;
- Papieren formulier in een box (op verschillende plaatsen, en die regelmatig worden leeggemaakt);
- Vaste momenten om over zichzelf en de dienst te spreken;
- Vertrouwenspersonen;
- Leidinggevenden.

Het is hierbij handig om te bepalen welke gegevens je bij zo'n melding wil verkrijgen, om in de mogelijkheid te zijn om deze te onderzoeken. Bij een online formulier kan je dit bijvoorbeeld verplicht zetten (zonder dat de melder zich verplicht dient te identificeren).
Voorbeelden van verplichte gegevens:

- Naam van de betrokkene waarover iets wordt gemeld;
- Gedrag dat werd opgemerkt;
- Moment dat dit werd opgemerkt;
- De plaats waar dit werd opgemerkt;
- De reden waarom de persoon die het heeft opgemerkt, twijfels heeft hierbij;
- …

Met deze basiselementen kan je verdergaan met een intern onderzoek, en deze informatie naar een hoger niveau doorgeven. Als er te weinig is om mee te starten, kan de vraag worden gesteld of het noodzakelijk is om verder te onderzoeken. Er moet over worden gewaakt dat gebrekkige informatie niet wordt aangevuld met veronderstellingen.

Informatie aan de melder

Het is belangrijk om te kijken welke informatie kan worden gegeven aan de melder (rekening houdend met de mogelijkheid dat de melder anoniem is of verder geen contact wenst hierover).

[4] 8 DECEMBER 2022. - Wet betreffende de meldingskanalen en de bescherming van de melders van integriteitsschendingen in de federale overheidsinstanties en bij de geïntegreerde politie

Een automatisch bericht of een overzicht van wat er vervolgens zal gebeuren, kan bijdragen aan een efficiënte communicatie en helpt bij het behouden van vertrouwen.

Daarbij kan men aangeven dat de informatie verder zal worden opgevolgd en dat dit geen gevolg heeft voor de melder. Als het achteraf om valse beschuldigingen blijkt te gaan, kan de melder hierop uiteraard worden aangesproken, om hem/haar te informeren en eventuele verdere stappen te nemen in het kader van het arbeidscontract, indien gewenst en mogelijk (onterechte meldingen kunnen eventueel als zware fout, bedrog, … worden aanzien).

Het is belangrijk om de werknemers van de installaties en de transporteurs te herinneren aan het feit dat het zo vroeg mogelijk observeren en detecteren van personen die mogelijk een interne dreiging kunnen worden, de mogelijkheid geeft om te reageren en om te voorzien in een individuele opvolging op een positieve manier.

B. Samenbrengen van informatie

Intern platform

De meldingen zelf komen het best op één centraal punt/platform om ervoor te zorgen dat alle meldingen op dezelfde manier kunnen worden behandeld en dat alle kanalen voor extra informatie duidelijk zijn. Het kan helpen om per binnenkomende melding een dossier te starten, juist om alle meldingen op dezelfde manier te behandelen en een overzicht te hebben van wat ermee wordt gedaan.

Men kijkt het best eerst naar de onafhankelijkheid. Indien iemand van het team dat de melding zal behandelen, te nauw betrokken is bij de melder of de betrokkene, dient te worden nagekeken of deze persoon deel kan blijven uitmaken van het intern onderzoek. Mede hiervoor is het gemakkelijker als er een kleine groep wordt gedefinieerd van verschillende diensten die een platform worden.

Daarbij, om de flexibiliteit van het mechanisme te bewaren, wordt de voorkeur gegeven aan een platform dat enkel bij elkaar komt op vraag van één van de leden, wanneer een individueel dossier dient te worden besproken. De rest van de tijd is dit platform ‘slapend’.

Daarnaast is het voor de goede werking ook noodzakelijk om een persoon te definiëren, binnen het platform, die verantwoordelijk is voor de opvolging, de coördinatie en begeleiding van de verschillende maatregelen die worden genomen.

Synthese van de melding of signalen

Alvorens een onderzoek te starten dient men het best na te gaan of de melding ontvankelijk is. Vragen die kunnen worden gesteld:

- Anonimiteit: kunnen we deze melding ook effectief nagaan?
- Betrokkenheid: bevindt de melder zich in de omgeving van de betrokkene zodat de melding oprecht kan zijn OF heeft deze melding een rechtstreeks positief gevolg voor de melder?
- Informatie: is er voldoende informatie of kan er meer informatie worden opgevraagd of opgezocht?

Wanneer er te weinig informatie is om mee verder te gaan, kan er worden besloten om op dat moment niet verder te gaan met een onderzoek. Dit zal ook samenhangen met een risicobepaling omtrent het wel of niet verderzetten van een onderzoek.

De ontvangen informatie dient zo sterk mogelijk te worden geobjectiveerd. Dit is een moeilijke oefening, want er wordt gevraagd aan mensen om hun observaties te melden, waardoor de ontvangen melding een gevoel van iemand kan weergeven of een situatie waarbij onrechtmatigheid wordt ervaren. Het doel is om de klacht zo objectief mogelijk te maken en te determineren waarover het gaat. Definiëren van categorieën van klachten kan hierbij ondersteunen, voorbeelden zijn:

- Verandering van gedrag
- Niet volgen van regels
- Meningsverschil
- …

Opvragen van basisinformatie

Zodra de melding verder zal worden onderzocht, kan het helpen om meteen enkele basisgegevens op te vragen voor verder intern onderzoek, bv.:

- Gegevens van HR;
- Eventuele klachten omtrent de persoon;
- Evaluatie van de persoon.

Een vast patroon (template of sjabloon) gebruiken voor het behandelen van klachten kan ondersteunen in de objectiviteit.

Deze informatie dient in het geval van onderaanneming eventueel te worden nagevraagd bij de veiligheidsofficier van het bedrijf waar de persoon tewerkgesteld is. Deze dient het best verder betrokken te worden bij het onderzoek, aangezien de veiligheidsofficier degene is die de bevoegdheid heeft om een intern onderzoek te voeren rond de mensen die in zijn/haar organisatie zijn tewerkgesteld.

C. Intern onderzoek

Een veiligheidsofficier heeft de bevoegdheid om over te gaan tot een intern onderzoek met betrekking tot het verzekeren van nazorg van de screening (art. 13/1 b van de wet van 11/12/1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen). Wanneer men overgaat tot een intern onderzoek, is het belangrijk om te kijken naar het risico dat de persoon kan vormen ten opzichte van de organisatie aan de ene kant, en de informatie die men over de betrokkene heeft langs de andere kant. De te nemen acties en het onderzoek naar de betrokkene dienen in proportie te zijn met de schade die hij/zij kan aanrichten.

Zodra een onderzoek lopende is, dient men natuurlijk die informatie te vergaren die nodig is om een gefundeerde beslissing te kunnen nemen. Hierbij kunnen verschillende acties worden genomen:

- Gesprek met de persoon en de melder: het is belangrijk om beide kanten te horen;
- Logging van gegevens van activiteiten;
- Gesprekken met collega's;
- Observatie van de persoon;
- Open source check;
- …

Dit onderzoek moet zoveel mogelijk gedocumenteerd worden, om als fundering te dienen voor eventuele acties. Hierbij dient rekening te worden gehouden met de vereisten omtrent privacy (toegang tot de informatie, bewaren van deze informatie, …). Het onderzoek zal dan ook even verregaand zijn als het risico dat de persoon kan vormen voor de organisatie. Dit intern onderzoek kan persoonsgegevens van de persoon verzamelen. Het gebeurt in dit geval in het algemeen belang van de organisatie en de wettelijke bevoegdheid van de veiligheidsofficier, al dient dit dus steeds te worden afgetoetst aan het proportionaliteitsprincipe.

De verzamelde informatie dient te worden geanalyseerd door de verantwoordelijken die instaan voor het intern onderzoek om te bepalen of de persoon een reële dreiging vormt ten opzichte van de organisatie.

D. Acties

Bij het begin van of tijdens het onderzoek

Afhankelijk van het risico dat de persoon vormt voor de organisatie, kan er worden beslist om reeds enkele preventieve acties te nemen bij het begin van het onderzoek:

- Toegang beperken;
- Extra begeleiding;
- …

Indien er wordt beslist om reeds acties te ondernemen, wordt hier het best duidelijk over gecommuniceerd naar de betrokkene. Men moet zich ervan bewust zijn dat dergelijke acties een persoon net verder afstand kunnen doen nemen of dat hierdoor het vertrouwen in de organisatie kan worden geschaad. Het is dus van belang om een zo open mogelijke communicatie te hebben. Er wordt dan het best gesproken met de betrokkene, zodat er meteen kan worden gesproken over de melding en de betrokkene de mogelijkheid heeft om zijn zienswijze toe te lichten.

Dit besluit kan ook worden genomen tijdens het onderzoek als gaandeweg uit de analyse blijkt dat het risico voor de organisatie groter lijkt.

Bij het nemen van concrete acties moet rekening worden gehouden met de proportionaliteit. Het nemen van concrete maatregelen kan een persoon verder duwen in de richting van een dreiging dan hij/zij in het begin van plan was.

Een bijkomende optie is om een extra onderzoek te vragen aan de Nationale Veiligheidsoverheid (NVO) op basis van elementen die al werden verzameld.

Na het onderzoek

Op het einde van het onderzoek zal er een conclusie worden getrokken: is er een mogelijke dreiging waarvoor verdere actie dient te worden genomen? Mogelijke acties zijn:

- Verdere opvolging;
- Extra beveiligingsmaatregelen, zoals begeleiding;
- Op een andere locatie tewerkstellen;
- Schorsing;
- Einde contract.

Indien er geen concrete dreiging is voor de organisatie zelf, maar de persoon wel in een situatie zit waarbij hij/zij hulp of ondersteuning kan gebruiken, is het aangewezen om te kijken wat de

organisatie hierbij kan doen; dit om het vertrouwen van de betrokkene te behouden na een eventueel onderzoek en hem terug op een positiever pad te brengen.

E. Rapportering intern (naar team/intern)

Bij een gegronde melding kan de betrokkene tijdens het onderzoek op de hoogte worden gebracht. Meestal gebeurt dat wanneer er met hem/haar een gesprek wordt opgestart. Bij de afronding van het intern onderzoek, dient aan de betrokkene een samenvatting van de conclusie te worden doorgegeven.

Indien mogelijk, kan het ondersteunend werken voor het meldingsproces dat er ook een contact is met de melder, zodat hij/zij op de hoogte is dat alles verder werd onderzocht en hoort of er al dan niet (zichtbare) maatregelen zijn getroffen. Hier dient men heel voorzichtig te zijn om niet te veel gegevens uit het onderzoek mee te geven, maar indien er zichtbare maatregelen zijn genomen, zal dit duidelijk zijn voor iedereen. Een communicatie naar het team van de betrokkene of de mensen waarmee hij/zij samenwerkt, kan hier duiding geven. De betrokkene dient namelijk in dat geval te werken onder extra maatregelen. Aangeven dat de organisatie nog vertrouwen heeft in de persoon (aangezien hij/zij nog tewerkgesteld is), maar dat er tijdelijk extra maatregelen worden genomen om de persoon te ondersteunen, kan de nodige context geven om zijn/haar werkzaamheden uit te voeren.

Men dient er hierbij het best rekening mee te houden dat een intern onderzoek op zich, met de al dan niet genomen/te nemen acties, een effect kan hebben op de betrokkene. Het vertrouwen van de betrokkene in de organisatie zal misschien geschaad zijn. Een dichtere opvolging door de manager is in dit geval eventueel aan te raden. Open communicatie tijdens het proces, met het nodige respect voor de betrokkene, kan daarbij veel ondersteuning bieden.

8. Continue verbetering

Dit proces van opvolging van werknemers dient regelmatig te worden geëvalueerd. Het gevaar bij dergelijke maatregelen is dat ervan uit wordt gegaan dat ze werken en dat hierdoor een zekere zelfgenoegzaamheid ontstaat met het systeem. Er wordt daarom aangeraden om een cyclus van permanente evaluatie in te bouwen waardoor deze maatregelen regelmatig worden herbekeken. Er kan met name een evaluatie worden gemaakt van:

- Het succes van de maatregelen (aantal onderzoeken, meldingen, incidenten);
- De *Security Culture*;
- Het niveau van ondersteuning van de maatregelen door de directie;
- De effectiviteit van de implementatie van de *'graded approach'*;
- …

Op dat moment kan men nagaan of bijkomende maatregelen kunnen worden genomen of eventueel minder succesvolle initiatieven kunnen worden aangepast.

Een dergelijke evaluatie geeft de mogelijkheid om *'awareness'* te verhogen en het succes van het aftercare-programma te herevalueren, om een continue verbetering in te bouwen die is aangepast aan de evolutie van de organisatie.

9. Conclusie

De *'insider threat'* is een reële dreiging voor de nucleaire sector. Deze dreiging is volledig bepaald door de werknemers die zich in de organisatie bevinden en de aard van de organisatie.

Het is daarom belangrijk om deze mensen op te volgen voor en tijdens tewerkstelling en bij beëindiging van het contract. In dit document hebben we getracht om de internationale richtlijnen ter zake te vertalen naar de Belgische situatie en dit met behulp van de nationale stakeholders. Door deze elementen af te toetsen met de personen die werkzaam zijn op het terrein, hebben we goede praktijken kunnen uitwisselen onderling in de sector, maar ook met andere sectoren. Het is duidelijk dat er geen *'one size fits all'*-oplossing bestaat voor het opvolgen van werknemers. De maatregelen dienen steeds gericht te zijn op de specifieke organisatie. Mede daarom werd ervoor gekozen om een overzicht te maken van de verschillende maatregelen die mogelijk lijken. De nucleaire installatie of vervoerder kan daarbij kiezen welke maatregelen de eigen organisatie zouden kunnen ondersteunen.

BIJLAGE A: Signalen die een indicatie zouden kunnen geven voor veranderend gedrag

Onderstaande kenmerken kunnen een indicatie geven dat een persoon gemakkelijker kan worden uitgebuit of onbetrouwbaar kan worden. Het vertonen van een van deze gedragingen is geen automatische indicatie dat iemand een insider-actie zal ondernemen, maar kan er gemakkelijker toe leiden. Deze factoren kunnen afhankelijk van de situatie wel zorgwekkend zijn. Daarnaast kan het vertonen van een van deze gedragingen misschien geen reden zijn tot verder onderzoek, maar als er meerdere elementen naar boven komen, kan dit worden herbekeken; des te meer wanneer het waargenomen gedrag de gewoontes van de persoon doorbreekt. Dit is dus een niet-exhaustief overzicht van mogelijke gedragingen die dienen te worden gerapporteerd:

Aanwezigheid:
- Verlaten van werkpost zonder toelating (als toelating vereist is)
- Herhaaldelijk misbruik van ziektedagen of ziek zijn voor langere periodes zonder duidelijk motief
- Frequent te laat zijn op het werk (terwijl dit vroeger geen gewoonte was)
- Specifieke en ongeloofwaardige excuses voor afwezigheid of laattijdigheid
- Frequente ongeplande korte afwezigheden (met of zonder ziektebriefje)
- Afwezigheid tijdens werkuren of moeilijk om gevonden te worden
- Veelvuldige aanvragen om het werk over te nemen van hem/haar

Productiviteit:
- Frequent missen van deadlines en afspraken zonder gegronde reden
- Onbetrouwbaarheid (bv. er kan niet worden vertrouwd op waar hij zegt te zijn of wat hij zegt te doen)
- Geeft onwaarschijnlijke excuses voor een slechte uitvoering van de werkzaamheden
- Vermijdt of doet het werk dat hem opgedragen is niet volledig
- Werk vereist grotere moeite of tijd dan is gepland
- Frequent fouten maken, slechte beslissingen of verkeerd oordeel
- Plotseling en meermaals vergeetachtig, wat een impact heeft op het werk
- Moeilijkheden om instructies op te volgen, onbegrip en onwil om de instructies te begrijpen

Emotionele stabiliteit
- Overgevoelig aan kritiek
- Koestert wrok en handelt hiernaar ten opzichte van medewerkers, leidinggevende en/of de organisatie
- Veelvuldige stemmingswisselingen
- Snel geïrriteerd
- Agressieve uitbarstingen
- Verhoogd geïrriteerd ten opzichte van medewerkers of anderen
- Ongewoon wantrouwend of paranoïde
- Overkomen als angstig, nerveus of paniekerig
- Ongewoon energetisch, lacherig, euforisch

- Depressief lijken, uitingen van hopeloosheid ten opzichte van zijn leven of zijn werk of van de maatschappij in het algemeen
- Besluiteloos, gebrek aan vertrouwen
- Plotselinge terugtrekking, isolatie van anderen zonder duidelijke aanleiding
- Apathie, afgenomen motivatie
- Afgeleid door familiale, financiële of wettelijke situatie of andere stresssituaties, moeilijkheden om om te gaan met de stress die hiermee samenhangt
- Zelfmoordneigingen of poging tot zelfdoding

Ongeoorloofd gedrag op de werkplaats
- Frequent defensief
- Verwijt anderen voor eigen problemen
- Veelvuldig liegen en overdrijven
- Klagen over medewerkers
- Bedreigingen uiten of intimideren van medewerkers
- Verhoogde irritatie over medewerkers of anderen
- Systematisch argumenterend, voor elke situatie of context
- Ongeoorloofde seksuele taal of gedrag
- Gedrag dat naast de context is of onvoorspelbaar
- Houdt zich niet aan de veiligheidsvoorschriften of volgt de procedures niet
- Onredelijk gedrag en onredelijke eisen ten opzichte van anderen
- Indicatie van bedrog, delinquent gedrag of gebrek aan betrouwbaarheid

Cognitieve achteruitgang
- Gedesorganiseerde gewoontes of werkritme
- Afgeleid, frequent dagdromen
- Gemakkelijk af te leiden, onmogelijkheid om gefocust te blijven
- Vertraagde bewegingen en reactietijd
- Problemen met kortetermijngeheugen
- Ongewone ideeën of gedachten
- Lijkt een slecht oordeel te hebben over toepassingen
- Lijkt niet te beseffen dat het voor hem/haar een stuk lastiger is om correct te werken, vindt het moeilijk om afstand te nemen
- Moeilijkheden om alert te blijven

Fysieke achteruitgang
- Veelvuldig uitgeput overkomen
- Persoonlijk hygiëne die achteruitgaat
- Meerdere fysieke klachten en ziekte
- Significant gewichtsverlies
- Lijkt zwak of achteruitgaande gezondheid
- Gehoorproblemen
- Fysieke trillingen
- Andere signalen van fysieke achteruitgang

Signalen van alcohol- of drugsmisbruik
- High of dronken lijken op het werk
- Ongewone spraakproblemen, desoriëntatie of gebrek aan coördinatie

- Slaperigheid of slapen aan het bureau
- Verbergen van drugs of alcohol in de wagen/op het werk
- De mogelijkheid om een grote hoeveelheid alcohol te drinken met minimaal effect, behoefte aan frequent gebruik van alcohol
- Onregelmatige werkuren
- Onverklaarbare, opeenvolgende afwezigheden op maandagen en/of vrijdagen
- Herhaalde en onsuccesvolle pogingen om geen drugs of alcohol te gebruiken
- Gebruik van drugs of alcohol voor omgaan met stress
- Misbruik van medicatie op voorschrift

Signalen van verandering in mentale status
- Onverklaarbare stemmingswisselingen
- Verhoogde nervositeit of angst
- Afnemen van prestatie of werkgewoontes
- Verandering in persoonlijke hygiëne
- Uitdrukking van ongewone gedachten, percepties of verwachtingen
- Patroon van onbetrouwbaarheid en liegen
- Poging om zichzelf te pijnigen, nood aan intense en gevaarlijke sensaties
- Ontevredenheid over werkgever of contractuele autoriteit/gezag

Respectloosheid en signalen van mogelijke agressie
- Argumentatief of beledigend gedrag ten opzichte van werkrelaties of familie dat tot discussies op de werkplaats of tot onderbrekingen van de werkzaamheden leidde
- De neiging om zichzelf te isoleren, verwerpen van sociale interactie, gebrek aan sociale ondersteuning, onverklaarbare en gemanifesteerde depressie
- Mondelinge uitbarstingen, meestal de aandacht brengen naar onderwerpen die niet direct gelinkt zijn aan het gesprek/werk
- Uitbuiting of mishandeling van anderen, meestal door intimidatie of machtsmisbruik
- Storend gedrag waarop raadgevingen van en supervisie door directie geen impact lijken te hebben
- Verbale of fysieke dreigingen ten opzichte van medewerkers of familie
- Extreme of herhaalde verklaringen die bitterheid, rancune of wraak vertonen
- Elk moment aanvatten voor geweld of het gooien van zaken
- Stalkgedrag
- Extreem of herhaaldelijk de regels of wetten breken
- Allerlei soorten misbruik

Signalen (of verdenking ervan) dat de medewerker in het criminele milieu actief is
- Diefstal of poging tot diefstal
- Fraude of poging tot fraude
- Partner- of kindermishandeling of -verwaarlozing
- Pogingen om anderen in illegale of verdachte activiteiten te betrekken

Signalen van misbruik van gevoelige informatie:
- Informatie doorgeven aan personen zonder toegang
- Vragen stellen over operaties en/of projecten waar de persoon geen toegang (meer) toe heeft
- Ongeoorloofde contacten met media

- Verzamelen of bewaren van gevoelig materiaal buiten de daartoe bestemde faciliteiten
- Lakse beveiligingsgewoontes (behandeling van gevoelige informatie via telefoon, geen gebruik maken van de locatie om gevoelige informatie op te bergen, op gevoelige informatie werken van thuis uit)
- Verklaringen of acties die demonstreren dat de persoon denkt dat de regels niet op hem/haar van toepassing zijn

Signalen van misbruik van computermogelijkheden
- Toegang tot databanken zonder toelating of zonder dat dit nodig is
- Ongeoorloofde zoekopdrachten/browsing door computerbibliotheken
- Ongeoorloofde vernietiging van informatie op databanken

Signalen van financiële kwetsbaarheid
- Onmogelijkheid om schulden af te betalen of niet-gerespecteerde regeling van schuldbemiddeling
- Compulsieve en herhaalde uitgaven
- Geen goede opvolging van de financiën of eigendommen van de organisatie

Signalen van samenspanning
- Leven/uitgaven buiten iemands financiële mogelijkheden
- Onverklaarbare of onverwachte grote sommen cash
- Onverwachte afbetalingen van schulden
- Verklaringen van grote sommen uit erfenis, rijke familieleden, cadeaus, investeringen, familiebedrijf, …
- Persoonlijke bezittingen die niet consistent zijn met het loon

Signalen van linken met verdachte derde partijen
- Het bezit en gebruik van een buitenlands paspoort
- Aanmoediging of verheerlijking van agressieve acties uitgevoerd door derde partijen of organisaties
- Associatie met of sympathie voor mensen en/of organisaties die deze acties aanmoedigen

Signalen van rekrutering
- Contact nemen/hebben met individuen die gekend zijn voor contacten of mogelijke contacten met buitenlandse inlichtingendiensten of terroristische organisaties
- Niet rapporteren van buitenlandse reizen
- Niet rapporteren van toenaderingen door buitenlandse organisaties
- Niet rapporteren van aanvragen voor gevoelige informatie naast de officiële kanalen
- Deel uitmaken van illegale activiteiten of gevraagd worden om hier deel van uit te maken

Signalen van verzamelen van informatie of verwijderen van materiaal
- Vragen krijgen over het verkrijgen van informatie of materiaal waartoe de persoon geen toegang heeft
- Handtekeningen vragen ter bevestiging van verwijdering van informatie of materiaal, zonder dat je de verwijdering hebt gezien

- Gebruik van niet-toegelaten apparatuur in zones waar gevoelige informatie of materiaal wordt bewaard, besproken of behandeld
- Gebruik van afluister- of observatieapparatuur in gevoelige of beveiligde zones
- Meenemen van gevoelige informatie of materiaal naar huis of andere niet-toegelaten locaties
- Toegang verkrijgen tot digitale gevoelige informatiesystemen zonder toelating
- Observeren van een medewerker die probeert toegang te verkrijgen tot gevoelige informatie of materiaal dat niet in lijn ligt met de werkzaamheden
- Ongewone interesse vertonen in informatie die ruimer gaat dan de huidige jobpositie
- Ongewone belangstelling of aanleg voor beveiliging
- Bewust peilen naar beveiligingsrespons

Signalen van een medewerker met criminele bedoelingen

- Probeert toegang te verkrijgen tot zones met gevoelige informatie door regelmatig vrijwilliger te zijn voor taken buiten de normale verantwoordelijkheden
- Overdadig gebruik van copy-, print- of andere toestellen om informatie te reproduceren of door te geven die buiten iemands taken valt
- Pogingen om collega's in situaties te lokken die hen in een compromitterende positie kunnen brengen
- Pogingen om collega's een verplichting op te leggen door middel van speciale behandeling, gunsten, geschenken, geld of andere middelen

Extra info “THE BEHAVIOUR BAROMETER: An Education and Awareness Tool”: BAROMETRE_EN_CPRLV_2016-1.pdf (info-radical.org)

BIJLAGE B: Link naar PHD-onderzoek met overzicht van maatregelen

Title	**Exploring insider threat awareness and mitigation: more than the devil in disguise**
Author	***Reveraert, Mathias***
Abstract	Employees that steal, commit fraud, sabotage, or leak confidential information: it is every employer's nightmare. Even though every public or private organisation – big or small – is vulnerable to so-called 'insider threats', this problem is too often overlooked because organisations assume that their employees can be trusted. Indeed, employees need to be trusted with access to the organizational assets because they need it in order to do their job. Still, this access implies that insiders are largely exempted from the security obstacles that external enemies have to overcome. Despite the fact that insiders can relatively easier threaten the organization's assets, they are often overlooked as potential threat. Belgium already encountered multiple insider threat incidents. The most striking example is the nuclear reactor Doel 4 that was deliberately sabotaged by an insider. More recent examples in Belgium are Jürgen Conings and Operation Sky. To on the one hand raise awareness on the insider threat problem, and on the other hand provide organizations with mitigation measures to better secure themselves against insider threats, research was done with the support from Brussels Airport Company, Bel-V, Elia, Engie-Electrabel, the Federal Agency for Nuclear Control and G4S on the insider threat problem. The results of the first part of the research provide us with insights on the awareness gaps of Belgian organizations concerning the characteristics of the insider threat as well as the ways to mitigate it. The results of the second part of the research give useful insights on what can be considered 'red flags' of insider threats that organizations should be vigilant of, as well as with mitigation measures that organizations can use to better secure themselves against insider threats.
Language	English
Publication	Antwerpen: Universiteit Antwerpen, Faculteit Sociale Wetenschappen, Departement Politieke Wetenschappen, 2023
Full text (open access)	https://repository.uantwerpen.be/docstore/d:irua:17211

BIJLAGE C: Tips & Tricks voor een gesprek[5]

When you have a doubt on someone's behaviour or changes in behaviour are noticeable, often the person isn't malicious, and it can be useful to talk to the person themself in order to have an idea of the reason. Information gathering is necessary in order to conduct a threat assessment. Data can be very useful, but to gather information on the intent or motivation, information from the person themself is of the biggest importance.

In general, you will gather more information if you can have an informal conversation (one on one), but it depends on the national legislation and your company culture whether this is possible. In some cases, you may need to have the conversation with a third party present. For example, it can help to have an objective view on what was discussed. In that case, it will be useful to prepare who will lead and who will observe (with a focus on how the person reacts and acts). Sometimes, the interviewed person may ask to have counsellors (advocate, union representatives…) with them.

Preparation of the meeting

°Gather the information you already have. You can use such information during the conversation, for example to substantiate or explain why you ask a question. Be sure to identify facts from assumptions and hearsay.

°During the meeting, you may want to offer support and help to the person: gather information on how you could do it in a concrete way.

°Make sure you know what you want out of the meeting: which information. The objective should be to "clear" the person by finding clear and innocuous explanations for suspicious elements.

°Check what kind of information you are legally authorized to ask. You may refer to regulations regarding private life, medical secrecy, anti-discrimination…

°Prepare (open) questions, to receive the needed information. Open questions may acquire more information.

°Leave your own perception out of your preparation, try to be as objective as possible. It could help to identify what your perception is in order to get it out of the questions/conversation. Try to keep an open mind and approach the meeting with good intent toward the person.

Invitation to the meeting

°Make sure you are in a place where you cannot be disturbed.

°An invitation to a planned meeting can be helpful, so the person cannot pretend to be needed elsewhere – but it might make the person suspicious → depends on company culture.

[5] IMPORTANT: These tips & tricks are appropriate for usual situations, when most of the time, people are not dangerous criminals and terrorists and, therefore, must be treated with respect and care. If you have proof or serious doubt on the fact that the person is malicious and/or dangerous, instead, you should contact your security service and police in a timely manner before deciding to carry an interview of the person. It could alert and give him/her an opportunity to commit a malicious act or to flee. It could also hamper a judicial investigation.

°Putting yourself in the position where you need help from the person, might help the conversation: 'Could we have a meeting, because I need your help with something'.

Meeting itself

°Inform the person on why you are having the meeting. You have information that needs to be clarified.

°Ask open questions.

°Talk from an "I" perspective. Avoid "you" sentences that are not perfectly factual or questions, because they can be interpreted as a judgment, and the person can feel threatened, and refuse to answer.

°Leave enough silences, so the person can answer and feels free to speak. Most people also tend to "fill the void" and give more information, even unexpected, when silence is given.

°Focus on the care for wellbeing of the person: 'Is there something we can help you with', 'I am concerned about your wellbeing'.

°Create a relaxing environment, so the person doesn't feel threatened.

°Look at the body language of a person. Try to observe.

°If you have doubt on the fact that the person is lying, you can insist on the fact that it is very important that the person is truthful. Information given may be checked and if it is found that the person has lied, it could have consequences.

°If the person seems distressed, try, and reinsure them that you are here to help them, to clarify the situation and, if needed, find solutions suitable both for them and for the service.

°Respect the person.

°Listen to what is being said and leave enough space for the person to talk. They should be talking more than you.

°Note all important elements. Verify with the person that you have well understood what they said.

After the meeting

°Try to make an objective analysis.

°Write down your initial thoughts, you can analyse them later, but the first impression is often the correct one.

°Check information provided by the person.

°If the person required help or support, act accordingly.

°If needed, contact your security service / the police.

BIJLAGE D: Omzendbrief CP3

Deze omzendbrief specifieert verder de bepalingen rond het klachtenbeheer van de politie.

Omzendbrief CP3: Omzendbrief van 29/03/2011 rondzendbrief cp3 betreffende organisatiebeheersing in de geïntegreerde politie, gestructureerd op twee niveaus (openjustice.be)

BIJLAGE E: Voorbeelden van opleidingen

Preventie van radicalisering:

- BeFUS - Preventie van gewelddadig extremisme op https://befus.be/2020/12/25/prevention-des-extremismes-violents/?lang=nl
- Handboek Lokale preventie en veiligheid in België op https://politeia.be/nl/artikels/290193-lokale+preventie+en+veiligheid+in+belgi%C3%AB
- VVSG - Rapport Radicalisering & Polarisatie (Ledenbevraging 2022) op https://www.vvsg.be/Publiek/VVSG%20Rapport%20Ledenbevraging%20Radicalisering%20Polarisering%202022.pdf
- Community Policing and the Prevention of Radicalisation (CoPPRa) – Internationale update 2021 op https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/collection-inspiring-practices/ran-practices/coppra_en

FANC

FEDERAAL AGENTSCHAP VOOR
NUCLEAIRE CONTROLE

Markiesstraat 1 bus 6A
1000 Brussel • België

www.fanc.fgov.be
meldpunt@fanc.fgov.be
+32(0)2 289 21 11

VERANTWOORDELIJKE UITGEVER
Frank Hardeman

April 2024