



Handreiking

Veiligheidszorg melden, registreren en Safety & Security Awareness

17 maart 2025



Inhoudsopgave

Deel 1: Achtergrond van Safety & Security	2
1.1 Fasen binnen Safety & Security	2
1.2 Safety Maturity Model van Hudson	3
1.3 De veiligheidspiramide van Heinrich	5
1.4 Melden en Registreren	6
1.5 Organisatie, techniek en mensen	7
Deel 2: aan de slag met uw veiligheidsbeleid	8
2.1 Preventie	9
2.2. Incident	10
2.3 Melding	11
2.4 Terugkoppeling.....	15
2.5 Opvang, nazorg en begeleiding	17
2.6 Analyse incident(en)	19
2.7 Registratie	20
2.8 Analyse cijfers en trends	22
2.9 Evalueren doelen	24

Deel 1: Achtergrond van Safety & Security

1.1 Fasen binnen Safety & Security

Binnen Safety & Security bestaan verschillende fasen, die samen een veiligheidsketen vormen. Elke fase heeft bijzondere kenmerken en een eigen aanpak.

1. Proactieve fase;
2. Preventieve fase;
3. Preparatiefase;
4. Repressiefase;
5. Nazorgfase.

Elke fase is gericht op een onderwerp in de gehele keten. Is een fase overgeslagen, dan vormt dit een zwakke schakel in de keten. In de fasegerichte aanpak komen allerlei zaken aan bod die te maken hebben met veiligheid, of dit nu overlast is van een groepje jongeren of de aanpak van ernstige feiten.

Proactieve fase

In de proactieve fase probeert u, door een structurele aanpak, oorzaken van agressie weg te nemen. Een voorbeeld is een groep hangjongeren die op het parkeerterrein rondhangt. U kunt deze groep aanpakken door u te beroepen op huisvredebreuk of het betreden van het terrein zonder toestemming. Maar eigenlijk zit u dan al meteen in de repressieve fase. Een alternatief is om samen met de ketenpartners (politie, gemeente, OM) deze groep beter in beeld te krijgen. Kijk wat u de hangjongeren kunt bieden om te voorkomen dat zaken escaleren. Daar liggen vaak mogelijkheden, meestal in combinatie met andere lopende veiligheidszaken in een gemeente. Hiermee voorkomt u dat het voor alle partijen vervelend wordt. Deze proactieve fase wordt steeds meer toegepast, met steeds betere resultaten.

Preventieve fase

Daarna probeert u in de preventieve fase om incidenten te voorkomen, door na te denken over verbetering van de veiligheid, de gezondheid en het milieu in de organisatie. Wat hebben we al en wat missen we nog in dit beleid? Denk hierbij vooral aan het delen van kennis op dit gebied met andere organisaties.

Preparatiefase

De verbetering van de veiligheid, gezondheid en het milieu doet u met organisatorische maatregelen, ondersteund door bouwtechnische en elektronische ontwikkelingen en nieuwe managementmethoden. In deze preparatiefase komen trainingen aan bod, zoals het omgaan met agressie, gedragsregels en gedragscode. Denk hierbij aan gastvrijheid en het uitdragen van positief opgestelde huisregels en gedragsregels. Hiermee geeft u duidelijkheid over gedrag dat niet wordt getolereerd.

Repressiefase

Zijn er dan toch nog personen die zich te buiten gaan aan agressief gedrag? Dan zijn de vooraf gemaakte afspraken met de ketenpartners, binnen de Publiek Private Samenwerking (PPS), een uitkomst. Die zijn bepalend voor de repressieve fase. Het is belangrijk dat u weet wat u van de politie, tijdens en na een incident, kunt verwachten. Discussies hierover dient u niet tijdens, of kort na een incident te voeren. De emoties spelen dan teveel op. Het werkt beter om vooraf afspraken te maken.

Nazorgfase

De opvang en nazorg voor slachtoffers en andere direct betrokkenen, staan centraal in de laatste fase. Op bepaalde afdelingen agressie-incidenten voor. De medewerkers die hier mee te maken krijgen zijn wel wat gewend, maar kunnen niet alles hebben. Ook zij kunnen op een punt belanden

waarin ze opvang en nazorg nodig hebben. Dat kan aan de heftigheid van een incident liggen, aan de frequentie, of aan persoonlijke omstandigheden. Goede opvang en nazorg kan er voor zorgen dat medewerkers toch met plezier naar hun werk blijven gaan.

Creëren van beleid

Het management van de organisatie dient duidelijkheid te verschaffen en richting te geven aan het veiligheidsbeleid en het beveiligingsbeleid. Bovendien hebben managers een voorbeeldfunctie naar medewerkers. Voor het veiligheidsbeleid houdt u rekening met alle mogelijke incidenten die onrust of schade kunnen veroorzaken. De werkgever dient maatschappelijke, technologische en wettelijke ontwikkelingen goed te volgen en, daar waar nodig, het beleid bij te stellen. Ook zaken als actiegroepen, calamiteiten en pers moeten goed geregeld te zijn. Hierdoor kunt u eventuele schade beperken of zelfs voorkomen.

Het integrale veiligheidsbeleid richt zich op:

- het voorkomen van risico's als gevolg van strafbaar, onoordeelkundig of slordig handelen van mensen (menselijke gedragingen);
- wettelijke kaders en overeenkomsten met derden;
- het waarborgen van de continuïteit van de organisatie en zo min mogelijke verstoring van het arbeidsproces;
- het waarborgen van de veiligheid van patiënten, cliënten, bezoekers en personeel.

U kunt hier op inspelen door bijvoorbeeld iedere maand op internet en in kranten te zoeken naar incidenten die bij organisaties hebben plaatsgevonden. Door een afweging te maken of een dergelijk incident ook in uw organisatie kan gebeuren, kunt u veel schade voorkomen. Natuurlijk is het niet de bedoeling om van de organisatie een bunker te maken waar niemand wil werken of verblijven. Het open karakter wilt u ongetwijfeld behouden. Toch kunnen bij een inventarisatie van incidenten verrassende zaken naar boven komen. Kijk daarbij goed naar de verschillen tussen beschermde gebieden, publiek toegankelijke gebieden en vitale gebieden. Toegangsbeperking van belangrijke gebieden, zoals de energievoorziening, de computercentrale of de operatiekamers, is (met uitleg van de reden) een heel probaat middel om incidenten te voorkomen.

Door op tijd de risico's te analyseren en met maatregelen te komen, kunt u incidenten voorkomen. Informeren van medewerkers over de maatregelen zorgt voor een verhoogd gevoel van veiligheid binnen de organisatie.

1.2 Safety Maturity Model van Hudson

Prof. dr. P.T.W. Hudson, hoogleraar binnen de cognitieve psychologie aan de universiteiten van Leiden en Delft, heeft een model gemaakt van de verschillende veiligheidsculturen. Hierin onderscheidt hij vijf verschillende veiligheidsculturen.

Een veiligheidscultuur van een organisatie is het product van individuele en groepswaarden, houdingen, competenties en gedragspatronen, die de betrokkenheid, stijl en vakkundigheid van veiligheidsprogramma's van die organisatie bepalen. Die cultuur kan zowel positief als negatief zijn.

De mate waarin een organisatie een veiligheidscultuur bezit, bepaalt in hoeverre men actief bezig is om veiligheid te borgen. Met het Safety Maturity Model geeft Hudson, op basis van verschillende kenmerken van een organisatie, een typering van de bedrijfscultuur.

De vijf culturen zijn:

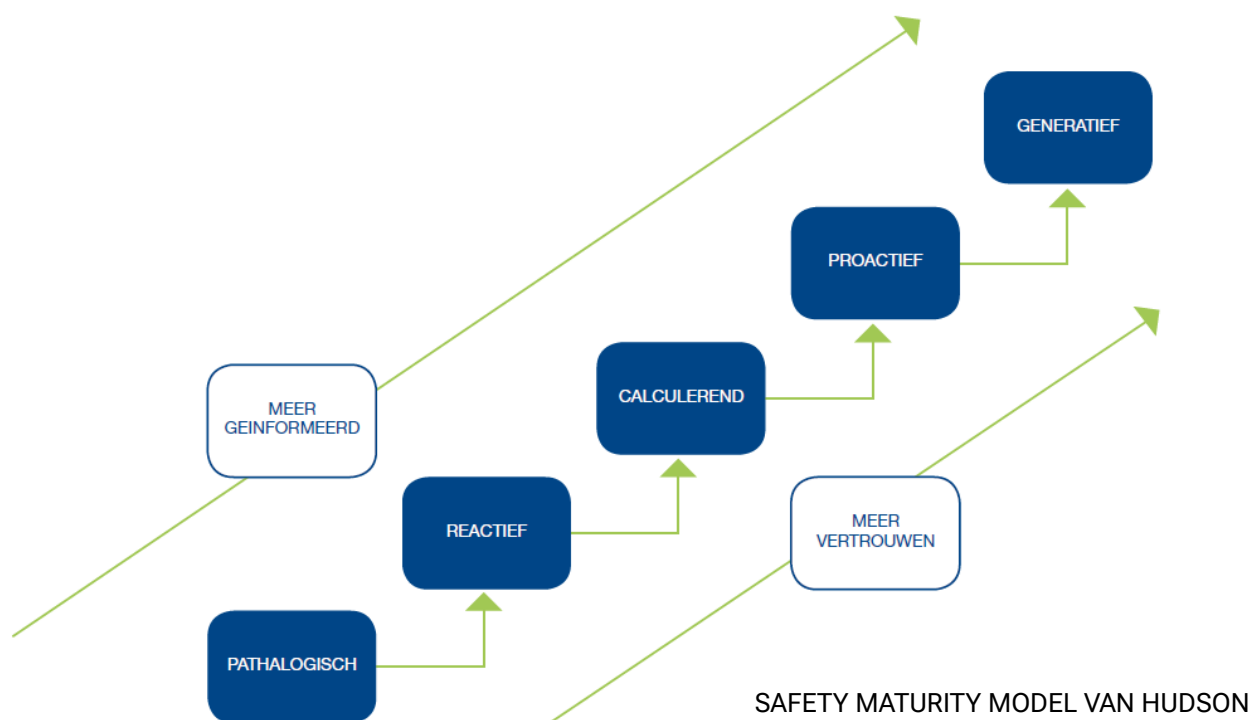
- 1. Pathologisch:
De enige zorg van de organisatie is om binnen de wettelijke kaders te blijven;
- 2. Reactief:
Veiligheid is voor de organisatie vooral na een incident belangrijk;
- 3. Calculatief:
Er is een systeem in de organisatie aanwezig om gevaarlijke situaties te managen;
- 4. Proactief:
Problemen in de organisatie worden actief opgespoord en (indien mogelijk) opgelost. Dit lijkt op de proactieve fase bij veiligheidsaspecten, maar is toch anders;

- 5. Generatief:
Er wordt op een goede en veilige manier binnen de organisatie gewerkt. 'Hier werk je veilig, of je werkt hier niet.'

Geïnformeerd zijn en vertrouwen

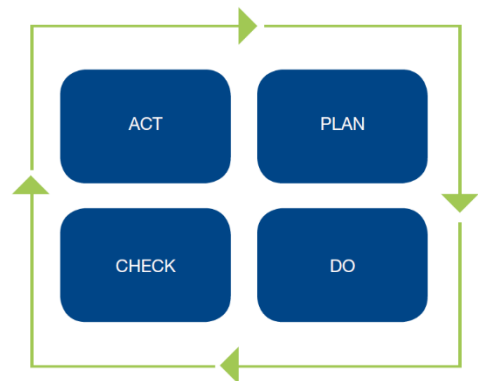
De vijf bedrijfsculturen van Hudson hangen onderling samen. Het model hieronder laat die samenhang zien. Het model is gebaseerd op de variabelen geïnformeerd zijn en vertrouwen. Het geïnformeerd zijn geeft aan in hoeverre medewerkers op de hoogte zijn van veiligheidskwesties en wat managers weten over zaken die spelen op veiligheidsgebied. Hoe beter de kwaliteit van communicatie over veiligheid, hoe beter de veiligheidscultuur. Grijp daarom alle mogelijkheden aan om het beleid op een positieve wijze te communiceren binnen de organisatie en te laten zien wat de resultaten van dit beleid zijn. Pas dan gaat security awareness leven en kan het worden geborgd in de organisatie. Zonder goede communicatie is er slechts sprake van incidentenmanagement.

De variabele vertrouwen heeft betrekking op het vertrouwen dat werknemers hebben in het management en andersom. Dit vertrouwen bepaalt of ongewenste gebeurtenissen gemeld worden en of werknemers actief verbetermogelijkheden aangeven. Samen geven beide variabelen een indicatie van de veiligheidscultuur. De vijf onderscheiden culturen liggen daarbij op één lijn, die een recht evenredig verband veronderstelt tussen de mate van geïnformeerd zijn en de mate van vertrouwen.



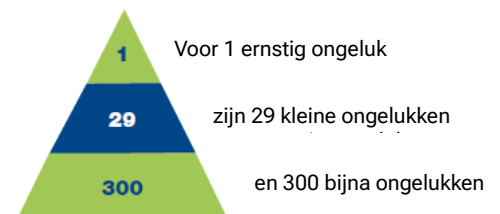
Kosten

Natuurlijk zijn er aan veiligheid kosten verbonden. De verhouding van veiligheid tot de totale bedrijfsvoering moet realistisch blijven. Toch blijft het voor medewerkers een vreemde en teleurstellende zaak wanneer er na een incident zaken goed geregeld en aangeschaft kunnen worden, terwijl dat daarvoor niet kon. Het is vele malen beter om een goede risico-inventarisatie of medewerkertevredenheidsonderzoek (MTO) te laten uitvoeren en incidenten vooraf te voorkomen. Overigens is een ander schema nog belangrijker: de PDCAcyclus van Dr. William Deming. Een beleidsplan maken is namelijk niet zo moeilijk, maar deze goed uitvoeren wel. U weet immers niet welke bedrijfscultuur in uw organisatie van toepassing is. Door bij elk veiligheidstraject een herhalende cyclus toe te passen, bent u constant bezig met het verbeteren van uw beleid.

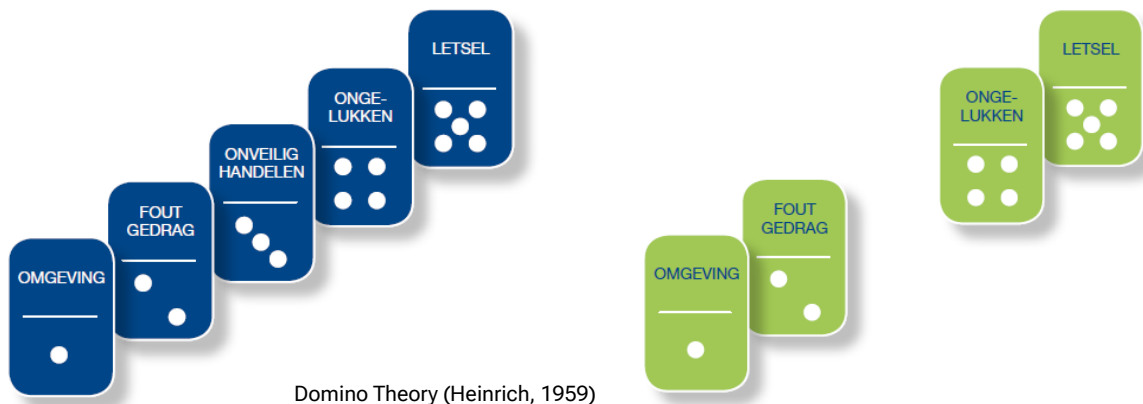


1.3 De veiligheidspiramide van Heinrich

Al in 1931 ontdekte veiligheidsdeskundige Herbert William Heinrich, die destijds voor een verzekeringsmaatschappij werkte, dat er een verband bestond tussen de ernst van ongevallen en de totale hoeveelheid ongevallen. In een eerste analyse van 75.000 ongevallen ontdekte hij een soort piramide van verschillende oorzaken. Toen hij opnieuw 50.000 ongelukken analyseerde, kijkend naar de gevolgen, formuleerde hij de legendarische 'Heinrich's Law'.



Heinrich ontdekte ook dat er een keten van 'basisvoorwaarden' bestaat, die als een soort domino-effect tot een incident kunnen leiden.



Heinrich zag de volgende keten:

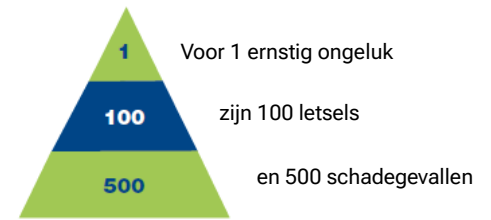
1. Door overerving en leren in de sociale omgeving worden personen gevormd;
2. Op basis van die vorming vertonen mensen fout gedrag;
3. Die fouten leiden tot onveilig handelen en onveilige omstandigheden;
4. Door dit handelen en die omstandigheden ontstaan ongelukken;
5. Ongelukken kunnen leiden tot letsel.

Hoewel er te discussiëren valt over de juistheid van de genoemde basisvoorwaarden, is de gedachtegang achter de dominotheorie hoopgevend. Elimineer één basisoorzaak en het incident kan niet meer voor komen. Sterker nog, een hele serie andere incidenten die gestoeld zijn op dezelfde basisvoorwaarden kunnen óók niet meer voor komen. Vergelijk het maar met de ingrediënten die er nodig zijn voor een explosie: een explosieve stof, in de juiste verhouding, met zuurstof en een ontstekingsbron, leidt tot een grote knal. Als je óf de explosieve stof, óf de zuurstof, óf de juiste mengverhouding, óf de ontstekingsbron weghaalt, kan er geen knal meer ontstaan.

Bird's Pyramide

Heinrich's theorie raakte in de vergetelheid totdat Frank Bird deze in 1969 nuanceerde. Bird analyseerde gedurende zeven jaar 90.000 incidenten bij een staalconcern en kwam tot een aangepaste piramide.

Bird paste deze piramide aan na een studie voor de International Safety Academy, over 1.753.498 incidenten bij 297 bedrijven. Deze analyse betrof 1.750.000 mensen en meer dan 3 miljard werkuren. Het resultaat van de studie toont opnieuw een 'ijsberg', waarbij het zichtbare deel (de ongelukken) klein is ten opzichte van het onderliggende deel (de incidenten).



Veel organisaties in de industrie en het transportwezen hebben hun incidenten geanalyseerd en steeds weer zien we de ijsberg opdoemen. Heinrich's Law leert ons dat hoewel elk incident tot serieus letsel kan leiden, de meeste dat niet doen. Zodra een incident kan ontstaan is het uiteindelijke gevolg grotendeels een kwestie van toeval. Doordat het overgrote deel van de incidenten niet tot rampen leidt, zijn we geneigd om onveilige beslissingen te nemen en onveilige situaties te accepteren. In veel organisaties treden domweg onvoldoende ernstige ongelukken op om daar iets aan te veranderen. In de zorg treden deze ongelukken wel op, maar door de aard van het werk en omdat ziekte, letsel en de dood er alom tegenwoordig zijn, vallen de 'ongelukken' in het eigen proces nauwelijks op. Of nog erger: ze worden gezien als een normaal verschijnsel. 'To err is human'.



Zou men kleinere incidenten identificeren en analyseren, dan zouden de 'basic risk factors' zichtbaar worden en zou men in staat zijn om de basis van de piramide te verkleinen. Hiermee neemt de kans op grotere incidenten evenredig af.

Conclusie

Heinrich leert ons dat het nauwelijks zin heeft om te sturen op de ernstige incidenten in de top van de ijsberg. Wel kun je zorgen dat de ijsberg lager wordt. Naarmate er drastisch minder kleinere incidenten plaatsvinden, neemt de kans op grotere incidenten evenredig af. Een zeer effectieve strategie daarin is het identificeren en elimineren van de 'Basic Risk Factors', oftewel het voorkomen van het domino-effect. Dat is de basis voor beheerste processen, waarin geen ruimte meer is voor ernstige afwijkingen.

1.4 Melden en Registreren

Zoals uit de Veiligheidspiramide in het vorige hoofdstuk blijkt: wil u iets doen aan het aantal en de ernst van de incidenten, dan is melden en registreren van die incidenten onontbeerlijk. Zonder analyse van eerdere incidenten kunt u niet veel beginnen en bent u bezig met incidentenmanagement zonder enige vorm van risico-inventarisatie.

Op een goede registratie van incidenten is een goede analyse mogelijk. Anders bent u alleen aan het registreren om het registreren. Analyse is het hoofddoel, maar vanzelfsprekend wordt een goede registratie ook gebruikt voor het monitoren van opvang, aangifte, etc. Met een goede analyse kunt u besluiten om het beleid aan te passen of maatregelen te nemen op organisatorisch, elektronisch of bouwkundig gebied. Het laat daarnaast de medewerkers zien dat er iets met hun meldingen is gedaan. Bovendien is het op termijn mogelijk om met een onkostenmodule¹ te laten zien dat het beleid ook financieel voordeel oplevert. Als het goed is gaan de kosten die worden veroorzaakt door incidenten na verloop van tijd omlaag.

Beleid op het gebied van security awareness is gericht op het veranderen en verbeteren van kennis, houding en gedrag van medewerkers en management ten aanzien van beveiliging. Dit is essentieel voor het invoeren van maatregelen op het gebied van veiligheid. Zonder het juiste gedrag van medewerkers zijn die maatregelen nagenoeg zinloos.

Een doelstelling kan zijn om het aantal ongewenste incidenten op verschillende gebieden terug te dringen. Denk hierbij aan risico's op het gebied van agressie, diefstal, vernieling, gevaarlijke stoffen of medicijnen.

Het belang van communicatie

Communicatie is bij Safety & Security Awareness essentieel. Een goede uitleg naar alle medewerkers zorgt er bijvoorbeeld voor dat zij hun personeelspas zichtbaar dragen en niet onder een jas of vest. Hierdoor is snel te zien of iemand zich ergens ophoudt waar hij eigenlijk geen recht toe heeft. Het zichtbaar dragen van de persoonlijke pas heeft meerdere voordelen: het verhoogt de herkenbaarheid van medewerkers, het geeft duidelijkheid, het haalt onbevoegden er snel uit, het verhoogt de rust op afdelingen, het verhoogt de veiligheid op afdelingen, het verhoogt het veiligheidsgevoel op afdelingen en het verbetert bij calamiteiten de herkenbaarheid van de BHV. Met goede communicatie maakt u duidelijk waarom maatregelen genomen zijn, waar de maatregelen zijn terug te lezen, wat de medewerkers er zelf aan kunnen doen en wat zij wel en niet moeten doen bij een gevaarlijke situatie. Insluipers worden hierdoor grotendeels buitengesloten. Communiceer op dit vlak niet alleen via intranet of eenmalige richtlijnen, maar geef uitleg op speciale bijeenkomsten. U kunt dan direct vragen beantwoorden. Na een eventuele aanpassing kunt u de richtlijnen vervolgens op intranet plaatsen.

1.5 Organisatie, techniek en mensen

Bij Safety & Security Awareness binnen een organisatie zijn drie onderwerpen belangrijk: de organisatie, de techniek en de mensen. Mensen met kwade bedoelingen zullen vooral gebruik proberen te maken van de zwakste schakel bij deze drie onderwerpen: de mens. Door een goede communicatie richting deze mensen (uw medewerkers) kunt u veel incidenten voorkomen. Drie belangrijke zaken moeten daarbij niet vergeten worden:

- medewerkers moeten inzien dat hun bijdrage zinvol is;
- mensen zoeken naar geborgenheid en verwachten dit van uw organisatie;
- mensen willen over zichzelf kunnen beslissen.

Dit kan alleen bereikt worden door een goede communicatie naar en met uw medewerkers. Daarnaast moet de techniek om de veiligheidstaak uit te kunnen voeren klantvriendelijk en up-to-date zijn en moeten de omstandigheden er naar zijn om de taak goed uit te kunnen voeren.

Als u start met een Safety & Security Awareness-programma, kan het verstandig zijn om aan te sluiten bij een al lopend communicatietraject, of om zelf een communicatieplan te (laten) maken. Teveel communicatietrajecten tegelijk leiden namelijk af.

TIPS

- Maak een soort tiplijn (bijvoorbeeld met een Tip van de week), zodat medewerkers na gaan denken over de veiligheid van hun werkomgeving. Beloon ze voor dit nadenken;
- Organiseer workshops over Safety & Security Awareness. Maak hierin duidelijk waarom er een veiligheidsbeleid wordt gevoerd en waarom bepaalde zaken zijn afgesproken;
- Probeer het veiligheidsbewustzijn te verbeteren door steeds een link te leggen naar de kwaliteit van het werk. Meer rust en tijd creëren namelijk ook kwaliteit;
- Safety & Security Awareness kan geborgd worden in een RI&E of een MTO;
- Vraag aan een lid van de Raad van Bestuur om ambassadeur te worden voor dit onderwerp en om mee te gaan naar de uitleg bij de medisch specialisten;
- Laat de medewerkers in workshops zelf voorbeelden noemen van maatregelen, met hierbij de reden voor de maatregel. Schrijf dit op een flap-over en ga de discussie aan met de groep;
- Vraag tijdens de workshop aan medewerkers wat ze nu anders gaan doen en laat ze dat opschrijven. Stuur dit na een x-aantal weken naar hen toe, met de vraag wat er van terecht gekomen is;
- Laat zien hoeveel geld er bespaard is doordat er minder incidenten zijn geweest;
- Loop een observatieronde op een afdeling en maak foto's. Bespreek deze tijdens een werkoverleg op de betrokken afdeling, maar laat de medewerkers eerst denken dat de foto's ergens anders zijn genomen;
- Maak met de veiligheidspiramide zichtbaar dat er toch incidenten plaats gaan vinden. Stel gewoon de vraag: 'Voor wie is het geluk op deze week?';

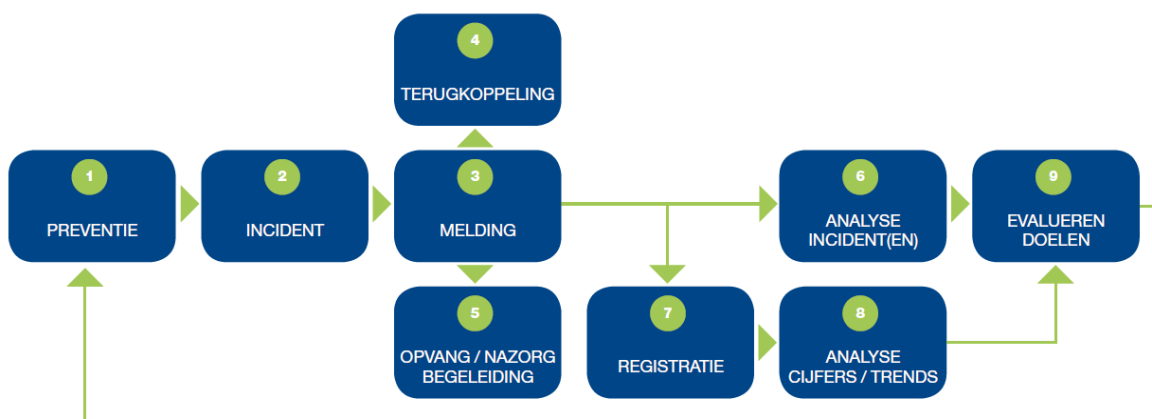
- Leer elkaar aan te spreken op gedragingen en leer medewerkers accepteren dat zij aangesproken kunnen worden.

Deel 2: aan de slag met uw veiligheidsbeleid

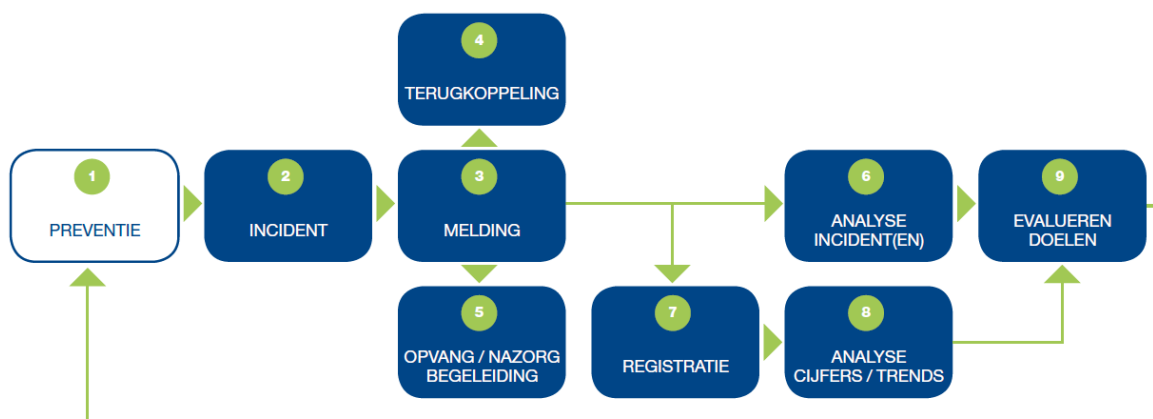
Leren uit incidenten

Dit deel van de handreiking begint met een schema waarin de verschillende stappen worden weergegeven van het leren uit incidenten. Daarna volgt per stap een toelichting. Centraal in het schema staan incidenten. Eigenlijk kan iedere uiting van agressie worden gezien als een incident. De ernst van incidenten kan echter heel verschillend zijn en variëren van onbeleefd gedrag tot fysieke mishandeling of doodsb bedreigingen. In hoofdstuk 2.2 bespreken we daarom wanneer er precies sprake is van een incident. Uit incidenten valt veel te leren. Ze staan vaak niet op zichzelf en meestal is er een aanleiding of een oorzaak binnen of buiten de organisatie. Ook zijn er vergelijkbare incidenten, met dezelfde oorzaak of aanleiding, en komen bij de ene persoon vaker incidenten voor dan bij de andere. In hoofdstuk 2.6 en 2.8 leest u hoe u van incidenten kunt leren door zowel het incident als de cijfers goed te analyseren. Die analyse kan echter pas plaatsvinden als de incidenten gemeld en geregistreerd worden. In hoofdstuk 2.3, 2.4 en 2.7 staan we daarom stil bij het melden en registreren en bij het terugkoppelen van de ingevoerde maatregelen. In hoofdstuk 2.5 gaan we in op het nabespreken van de incidenten, als onderdeel van opvang en nazorg. Ten slotte laten we in hoofdstuk 2.9 zien hoe u met behulp van de cijfers doelen kunt evalueren en bijstellen.

Om incidenten te voorkómen is proactief beleid nodig. Gastvrijheid heeft zijn prijs, maar ook zijn grens. Daarvoor dient u te weten waardoor agressie kan ontstaan, wat u kunt doen om dit te voorkomen, wat de huisregels zijn en hoe u hierover communiceert. Een registratiesysteem kan inzicht geven in oorzaken van agressie en duidelijk maken hoe vaak een bepaalde oorzaak voorkomt. Ook om te weten of de maatregelen die u neemt echt effect hebben, zijn cijfers nodig. De volgende stap is preventie. Daarbij gaat het om het nemen van maatregelen in situaties waarin agressie kan ontstaan. Repressie is nodig als er al sprake is van agressie. Het gaat dan om het daadwerkelijk optreden tegen de veroorzaker, bijvoorbeeld door de beveiliging of de politie. Met een goed registratiesysteem krijgt u bijvoorbeeld inzicht in het aantal waarschuwingen, het aantal toegangszonzeggingen en het aantal aangiftes.



2.1 Preventie



Het uiteindelijke doel van preventie is het voorkomen van agressie. Om agressie te voorkomen is het belangrijk om te weten waardoor het ontstaat. Agressie kent in hoofdlijnen vier vormen:

Expressieve agressie

Dit is het (luidruchtig) uiten van ongenoegen en is gericht op de situatie en op de organisatie. Het kan eenvoudig escaleren tot frustratie-agressie. In dit geval kunt u het beste begrip tonen.

Frustratie-agressie

Dit zijn frustraties over de dienstverlening of over de procedures. De emoties kunnen bij de agressor snel oplopen en hij heeft steeds minder controle over zijn eigen gedrag. De agressor kan alle stadia van emotie doorlopen. Ook hier is het belangrijk dat u begrip toont en vooral dat u de agressor serieus neemt. De agressie is niet persoonlijk gericht.

Instrumentele agressie

Deze vorm van agressie is op de persoon gericht en wordt heel bewust geuit. De agressor heeft volledige controle over zijn eigen gedrag. Advies: probeer heel consequent over te komen en aan de agressor duidelijk te maken dat dit gedrag hem niet helpt om zijn zin te krijgen.

Onbeheerste agressie

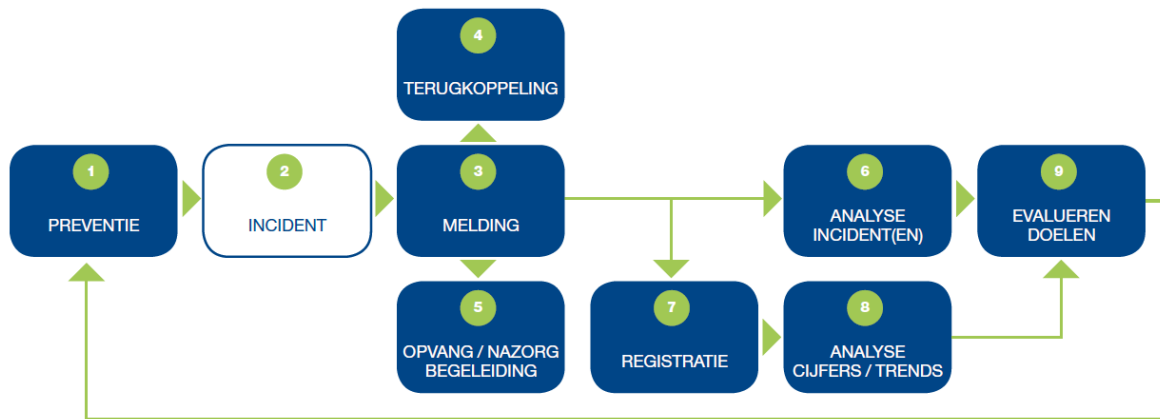
Onbeheerste agressie heeft vaak een verslaving van drank, drugs of een psychische stoornis als oorzaak. De agressor is onvoorspelbaar, snel gewelddadig en ontbeert rationaliteit. Roep in dit geval zo snel mogelijk hulp in van beveiliging of politie en houd zoveel mogelijk afstand.

Het is belangrijk dat medewerkers het soort geweld (h)erkennen en daar naar handelen. Een training helpt hen hierbij. Als u onderzoek doet naar de oorzaken van agressief gedrag en de mogelijkheden om dit aan te pakken, helpt het om doelen te stellen. Die doelen moeten dan wel SMART₂ geformuleerd worden. U kunt doelen op verschillende niveaus vaststellen: binnen het team, een afdeling, een cluster, een divisie of de hele instelling.

Mogelijke doelen

- Minder incidenten;
- Minder ernstige incidenten;
- Meer tevredenheid onder medewerkers over opvang en nazorg;
- Meer tevreden (minder gefrustreerde) patiënten en cliënten;
- Meer medewerkers die zich veilig voelen;
- Minder schade bij medewerkers (psychisch, fysiek en materieel);
- Minder verzuim als gevolg van incidenten;
- Minder verlies aan werktijd door incidenten;
- Minder kosten door vernieling, diefstal en vandalisme.

2.2. Incident



Wanneer is er sprake van een incident? Zoals we al in de inleiding hebben gezegd: eigenlijk is elke situatie waarin sprake is van ongewenst gedrag een incident. Daar hoort ook onbeleefd of grof gedrag bij, of ongewenst seksueel (getint) gedrag. Niet alle incidenten gaan samen met agressief gedrag, maar ze kunnen wel leiden tot agressie. Een organisatie kan er daarom voor kiezen om ook aan niet-agressieve incidenten aandacht te besteden. Zo wordt het werk voor de medewerkers aangener en plezieriger.

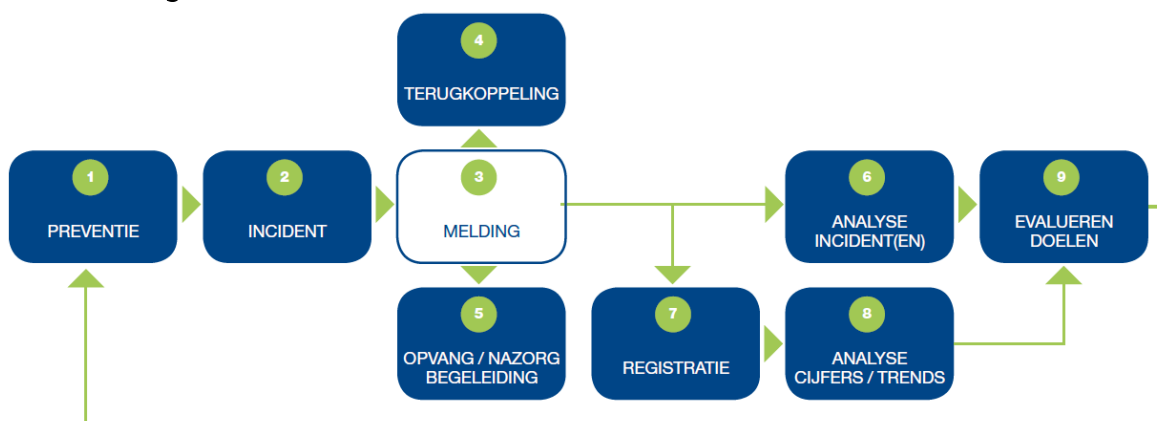
Waarden-en-normen discussie

Tijdens het project Veiligezorg® wordt in de organisatie (vaak op alle afdelingen) een 'waarden en normen'-discussie gevoerd. De bedoeling daarvan is om samen te komen tot correcte en prettige omgangsvormen. Deze gelden voor zowel medewerkers onderling, als naar patiënten en cliënten toe. Met deze omgangsvormen kunt u gedragsregels (ook wel huisregels) opstellen voor alle patiënten en bezoekers. Aan deze gedragsregels kunt u een sanctioneringsbeleid koppelen, met een waarschuwing, een toegangszegging, een schadevergoeding, een aangifte, of het stopzetten van de zorgverlening. De huisregels dient u duidelijk kenbaar te maken aan bezoekers en patiënten. U kunt ook een gedragscode opstellen voor medewerkers, waaraan weer een heel ander sanctioneringsbeleid (conform de HRM-regels) kan worden opgesteld.

Niet-agressief gedrag

Tijdens de 'waarden en normendiscussie' geven veel medewerkers aan dat ze ook niet-agressief gedrag (zoals onbeleefd of ongeduldig gedrag) erg vervelend vinden. Toch accepteren ze dit gedrag vaak wel. Hun verklaring: 'Dat hoort er gewoon bij tegenwoordig.' Maar ook gastvrijheid kent zijn grenzen. Bij verbale of non-verbale agressie is het echter lastig om duidelijk een grens aan te geven. Ook is het lastig om het er samen over eens te worden wanneer die grens overschreden wordt. Daardoor is het vaak veel moeilijker om medewerkers zo ver te krijgen dat ze deze situaties melden. In veel organisaties lopen al projecten in het kader van klantvriendelijkheid, waarbij ook aandacht wordt besteed aan bejegening. Door in de communicatie naar medewerkers toe een koppeling te maken tussen dit project en de aanpak van agressie, kunt u beide onderwerpen versterken gesteld.

2.3 Melding



Wat is melden? En wat is precies het verschil tussen melden en registreren? Melden is aangeven dat er een incident is geweest. Dat kan mondeling, schriftelijk of digitaal gebeuren. Daarbij moet altijd een aantal gegevens worden doorgegeven.

Het schriftelijk melden van een incident is overigens niet hetzelfde als registreren, ook al worden er gegevens genoteerd op een meldingskaart of meldingsformulier. Registreren betekent het opnemen van een incident in een formeel registratiesysteem. In dit hoofdstuk gaan we dieper in op het melden van incidenten en op manieren waarop u medewerkers kunt stimuleren om incidenten te melden.

Definitie

Het melden, registreren en analyseren van incidenten houdt in: het opzetten en invoeren van een procedure voor het melden, registreren en analyseren van agressie- en geweldsincidenten, op grond waarvan verbeteringen kunnen worden ingevoerd. Hierbij moet voor het personeel duidelijk zijn wat er wel en niet onder agressie- en geweldsincidenten wordt verstaan. Over de resultaten van de analyse en de daaruit voortvloeiende acties moet terugkoppeling plaatsvinden naar de melders.

Waarom?

Om agressie en geweld doeltreffend aan te pakken moet de werkgever bekend zijn met voorvallen die binnen de organisatie plaatsvinden. U weet pas wat er organisatie breed gebeurt met agressie- en geweldsincidenten als de voorvallen gemeld en vervolgens geregistreerd worden. Of u nu via een digitaal systeem of via een ander systeem voorvallen meldt en registreert, het vastleggen van incidenten geeft inzicht in de aard en omvang van de voorvallen en biedt input voor het (bij)stellen van het veiligheidsbeleid. Melden zorgt ervoor dat benodigde informatie aan collega's bekend wordt, waardoor zij zich in de toekomst beter kunnen voorbereiden. Het melden van voorvallen is het startsein tot directe opvang van het slachtoffer en eventuele getuigen van het voorval.

Er is een aantal belangrijke redenen om incidenten te melden:

- **De opvang van, en de nazorg aan medewerker(s) kort na het incident:**
Als een incident gemeld wordt, is het bekend bij de leidinggevende. Die kan vervolgens voor opvang en nazorg zorgen. Ook na een aantal dagen of weken is aandacht voor het welzijn van de medewerker nog belangrijk.
- **Het nabespreken van incidenten:**
Het nabespreken van een incident met de betrokkenen kan helpen om het gebeurde te verwerken. Ook kan het opheldering geven bij vragen en onduidelijkheden tijdens of na het incident.
- **Extra ondersteuning voor medewerkers die dat nodig hebben:**
De ene medewerker heeft meer moeite om met agressieve situaties om te gaan dan de andere. Door incidenten te melden wordt dit duidelijk. Daardoor kunnen medewerkers die dat nodig hebben extra ondersteuning krijgen, bijvoorbeeld via een training of met tips van collega's.
- **Het leren uit incidenten:**
Het is erg zinvol en leerzaam om regelmatig één of meerdere incidenten te analyseren en daarbij te kijken naar alle aspecten voor, tijdens en na het incident³.
- **Het opstellen, evalueren en aanpassen van beleid:**
Veel organisaties hebben naar aanleiding van incidenten een veiligheidsbeleid ontwikkeld. Daar

horen ook verschillende maatregelen bij. Of die maatregelen daadwerkelijk effect hebben, is vooral te zien aan het aantal (en de ernst van) incidenten ná de invoering ervan. Ook kunt u monitoren of er herhaling plaats vindt, wat betreft het incident of de veroorzaker.

- **Verplichting van het ministerie van Sociale Zaken en Werkgelegenheid:**

De overheid heeft in de Arboret laten opnemen dat organisaties verplicht zijn om een beleid te voeren dat gericht is op het beschermen van hun werknemers tegen agressie en geweld en tegen de nadelige gevolgen daarvan. Dat beleid wordt door de Inspectie SZW (voormalige Arbeidsinspectie) gecontroleerd.

Wat moet u precies melden?

In het vorige stuk hebben we al beschreven wanneer we het hebben over een agressie-incident. Die situaties moeten altijd worden gemeld. Het melden van verbale agressie is vaak lastig. Deze vorm van agressie komt in sommige organisaties zoveel voor dat het bijna als gewoon wordt gezien. Dat is het natuurlijk niet. Met discussies over waarden en normen maakt u medewerkers er bewust van dat verbale agressie niet normaal is en dat zij in die gevallen eerder hun grenzen en die van de organisatie moeten aangeven. Die bewustwording komt niet van vandaag op morgen, maar kan wel leiden tot resultaten op langere termijn. Het is noodzakelijk dat afdelingen afspreken om ook verbale agressie te melden.

Een werkgever voert een goed beleid op het gebied van agressie en geweld als:

- Er maatregelen zijn genomen op het gebied van voorlichting en opleiding;
- Er protocollen zijn voor werkzaamheden met risico op agressie en geweld;
- Er een meldingsprocedure is voor gebeurtenissen die samengaan met agressie en geweld;
- Incidenten met agressie en geweld worden besproken, bijvoorbeeld tijdens een werkoverleg;
- Er procedures zijn voor de opvang en begeleiding van werknemers die geconfronteerd zijn met agressie of geweld;
- Er materiële, bouwkundige of organisatorische maatregelen zijn genomen om agressie en geweld te voorkomen;
- Eventuele risico's op agressie en geweld zijn opgenomen in de RI&E en eventuele daaruit voortvloeiende maatregelen in het plan van aanpak zijn vermeld (het liefst met vermelding van de termijnen waarbinnen de maatregelen gerealiseerd worden).

Een manier om tot afspraken te komen over het melden van verbale agressie, is om verbale agressie minstens twee maanden lang (heel simpel) op de afdeling te registreren. Daarna kan de afdeling de meldingen bespreken en afspreken wat er voortaan gemeld gaat worden en waarom. Het beste is om dat niet woordelijk te doen, maar op themaniveau. Denk bijvoorbeeld aan discriminerende opmerkingen of seksueel getinte opmerkingen (seksueel intimiderende opmerkingen moeten altijd gemeld worden; deze vallen onder intimiderend gedrag). Als het niet lukt om afspraken te maken, dan kan het helpen om een waardendiscussie te voeren. Daarbij kunt u de vraag stellen waarom medewerkers niet willen melden. Dat kan bijvoorbeeld te maken hebben met een gevoel van onveiligheid naar de eigen organisatie.

Het slachtoffer of de getuige van een agressie- of geweldsvoorzak geeft in de melding duidelijk aan:

- Wie er bij het incident betrokken was;
- Wat er gebeurde;
- Waar het gebeurde;
- Waarom het gebeurde;
- Wanneer het gebeurde;
- Waarmee het gebeurde;
- Op welke wijze het gebeurde.

Wanneer moet u iets melden?

Het komt vaak voor dat medewerkers denken dat wanneer de beveiliging en/of politie erbij is geweest, ze niets meer hoeven te melden. Het is dus belangrijk dat u uitlegt waarom dat toch nodig is.

(non)verbaal geweld	Fysiek geweld	Discriminatie	Seksuele intimidatie	Overige intimidatie
<ul style="list-style-type: none"> • schreeuwen • schelden • vernederen • treiteren • pesten • vals beschuldigen 	<ul style="list-style-type: none"> • duwen, trekken, slaan • vastgrijpen • schoppen • gooien met voorwerpen • vernielen van voorwerpen • fysiek hinderen • spugen • diefstal van eigendommen • verwonden • roofoverval • geven van een kopstoot • bijten 	<ul style="list-style-type: none"> • naar huidskleur • naar sekse • naar leeftijd • naar geloofsovertuiging • naar seksuele geaardheid of voorkeur • etc. 	<ul style="list-style-type: none"> • seksueel getinte opmerkingen • seksueel getinte blikken • nafluiten • exhibitionisme • aanranding • seksueel getinte e-mail of sms • seksuele chantage • hijgers • verkrachting • seksuele handtastelijkheden 	<ul style="list-style-type: none"> • dreigen • bedreigen • onder druk zetten • bedreigende gebaren maken • chanteren • bekladden • dreigbrief of e-mail • gezinsleden bedreigen • stalken • achtervolgen • bommelding • wapengebruik

Medewerkers moeten weten dat melden niet alleen belangrijk is voor het verzamelen van cijfers, maar ook om eruit te kunnen leren en om persoonlijke aandacht te kunnen krijgen na het incident. Goed beleid zorgt ook dat zorgmedewerkers altijd incidenten melden. Met meldingen kunnen ook veroorzakers van agressie worden aangepakt. Lang niet iedereen is agressief vanuit een ziektebeeld. Sommigen gebruiken agressie om (bijvoorbeeld) snel geholpen te worden. Door incidenten goed te melden komen dergelijke personen in beeld en kunt u hen aanspreken op hun gedrag. Dit kan ook via de gemeente, die bijhoudt of mensen zich frequent agressief gedragen tegen medewerkers met een publieke taak. Door anderen niet aan te spreken op hun gedrag en door incidenten niet te melden, accepteren werknemers eigenlijk dat de veroorzaker zich ook misdraagt naar hun collega's.

De meldingsprocedure

In een meldingsprocedure staat wat medewerkers precies moeten melden, hoe ze kunnen melden en naar wie de melding toe moet. Uit de gegevens van een aantal organisaties blijkt dat de meldingsprocedures soms problemen opleveren. De belangrijkste zijn:

- Onbekendheid met het meldingsprotocol;
- Onduidelijkheid over hoe precies moet worden gemeld;
- Geen of weinig gebruik van het intranet;
- Veel (papier)werk;
- Tijdgebrek bij de medewerkers;
- Te weinig tijd bij leidinggevenden om voldoende aandacht te besteden aan het melden.

Mogelijkheden om in dat geval de meldingsprocedure te verbeteren zijn:

- Een herkenbaar en eenduidig meldingssysteem;
- Een digitale meldingsprocedure;
- De mogelijkheid om vanuit huis, via internet, te kunnen melden;
- Eén vast incidentenmeldpunt via het intranet;
- Een snelle en efficiënte meldingsprocedure;
- Het opnemen van de meldingen in een geautomatiseerd kwaliteitssysteem;
- Het invoeren van veiligheidscoaches op de afdelingen, die hun collega's kunnen adviseren. Dit kunnen ook beveiligers zijn die als aanspreekpunt fungeren voor een afdeling.

Hoe melden?

Vanuit het oogpunt van de medewerker is de ideale meldingsprocedure een procedure waarbij medewerkers zo min mogelijk hoeven in te vullen en waarbij ze zo snel mogelijk (binnen een dag) een terugkoppeling krijgen van hun leidinggevende. Het gebeurt echter nog wel eens dat de praktische kant van een meldingsprocedure belangrijker wordt gevonden dan de menselijke kant. In dat geval wordt direct om alle informatie gevraagd, zodat er geen contact meer hoeft te worden opgenomen met de medewerker voor het aanvullen van ontbrekende gegevens. Maar daar gaat het melden juist om: dat de leidinggevende, meteen na de melding, persoonlijk contact opneemt met de medewerker. De leidinggevende kan dan horen hoe het gaat en zo nodig opvang, begeleiding en nazorg regelen.

Veiligezorg® geeft een procedure de voorkeur waarbij:

- Het voor de medewerker zo gemakkelijk mogelijk is om een melding te doen;
- Zo snel mogelijk contact wordt opgenomen met de medewerker.

Veiligheidscoaches

Wanneer er op een afdeling veiligheidscoaches zijn, dan kunnen zij een belangrijke rol spelen bij het motiveren van collega's om te melden. Ook kunnen zij de leidinggevende informeren, helpen bij het verzamelen van aanvullende informatie, een nabespreking initiëren, of informatie terugkoppelen naar het slachtoffer.

Wat kunnen redenen zijn om niet te melden?

- Agressie hoort nu eenmaal bij het werk;
- Ik zie incidenten vaak niet als een probleem;
- Ik heb er geen last van; ik ben het gewend;
- Het is niet tegen mij persoonlijk gericht;
- Er is toch weinig aan te doen;
- Als ik er aandacht aan besteed, escaleert het juist eerder;
- Het is me niet duidelijk wat wel en wat niet gemeld moet worden;
- Ik vind niet alles ernstig genoeg;
- Er komen zoveel incidenten voor, dan *blijfik* melden;
- Het is me niet duidelijk wat voor nut het heeft om te melden;
- Ik heb geen zin om er tijd aan te besteden, ik heb het al druk genoeg;
- Collega's vinden het overdreven als ik me daar druk om maak;
- Als collega's niet of nauwelijks melden en ik meld wel, dan lijkt het of ik degene ben die altijd last van agressie heeft en denken ze dat het aan mij ligt;
- Ik moet weerbaar en psychisch stabiel zijn; melden is een teken van instabiliteit of verminderde weerbaarheid;
- Ook al meld ik het, ik hoor er toch nooit meer iets over terug.

Melden via intranet

Steeds meer organisaties hebben een procedure ontwikkeld waarbij meldingen digitaal, via intranet, kunnen worden gedaan. Dat heeft voordelen, maar ook nadelen.

Voordelen:

- Formulieren raken niet op en hoeven niet aangevuld te worden; Anderen, zoals de leidinggevende of degene die de meldingen in het registratiesysteem invoert, kunnen meteen digitaal geïnformeerd worden;
- Het systeem is altijd beschikbaar;
- De gegevens hoeven niet opnieuw ingevoerd te worden;
- Er kan direct een digitale terugkoppeling aan de medewerker worden gegeven zodra de melding binnen is.

Nadelen:

- Medewerkers die niet zo gemakkelijk toegang tot een computer met intranet hebben moeten meer moeite doen;
- Het is niet altijd gemakkelijk om het meldingsformulier op intranet te vinden;
- Als er geen kopie van de melding naar de leidinggevende gaat, kan deze geen aandacht aan de medewerker schenken. Oplossing: de melding wordt primair naar de leidinggevende gestuurd met een kopie naar de arboafdeling, zodat het vervolg ook gemonitord kan worden;

- Vaak moeten medewerkers veel te veel informatie invullen, wat hen ervan weerhoudt om een melding te doen.

Oplossingen:

De nadelen van digitale meldingen via intranet kunnen worden ondervangen door:

- De meldingsprocedure zo in te richten dat er behalve een digitale terugkoppeling ook een persoonlijke terugkoppeling door de leidinggevende plaatsvindt;
- Medewerkers die bezwaar hebben tegen digitaal melden de mogelijkheid bieden om een melding te doen met een meldingskaartje of een formulier;
- Het meldingsformulier gemakkelijk vindbaar maken. De melding integreren in een digitaal formulier dat ook gebruikt kan worden voor andere meldingen (zoals VIM, MIP, etc.);
- Na het verzenden van de melding krijgt de medewerker direct een pop-up scherm te zien, waarin staat dat de melding in goede orde is ontvangen en dat er contact met de medewerker wordt opgenomen.

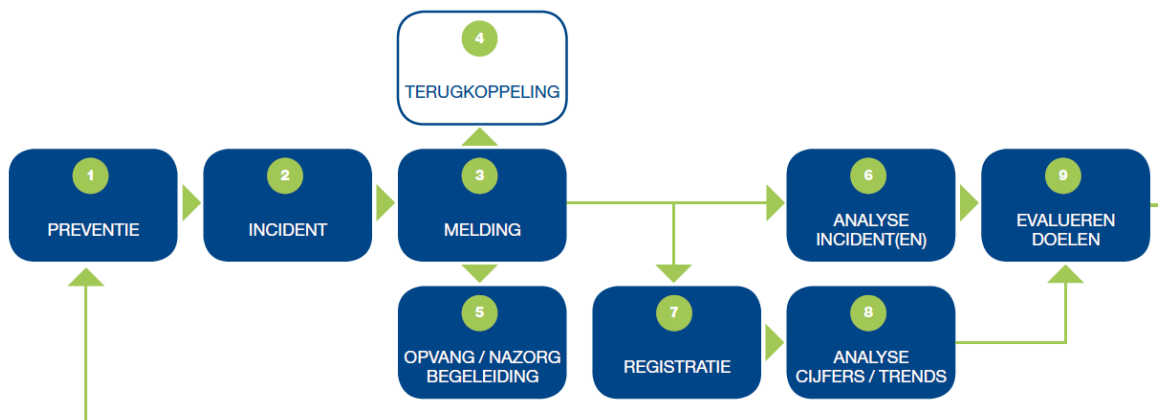
Bij wie melden?

Naar wie de melding precies gaat is op zich niet zo belangrijk. Een inventarisatie door Veiligezorg® laat zien dat er verschillende functionarissen zijn waar de melding naar toe kan worden gestuurd. Denk aan de teamleider beveiliging, de teamleider van de eigen afdeling, de leidinggevende, de Weekend- Avond- Nachtdienstcoördinator (WANco), de arbo- of veiligheidscoördinator, de adviseur arbeidsomstandigheden, of de vertrouwenspersoon.

Een medewerker moet altijd aan kunnen geven dat hij niet wil dat de leidinggevende informatie krijgt over de melding. Dat kan bijvoorbeeld relevant zijn wanneer de leidinggevende een rol heeft gespeeld bij het incident.

Wat wél belangrijk is, is dat de melding binnen 24 uur bij de leidinggevende terechtkomt. Verschillende organisaties hebben dat in hun procedure ingebouwd. De ontvanger van de melding zorgt voor de terugkoppeling naar de leidinggevende. Bij een digitale melding kan dat in het systeem worden ingebouwd, bijvoorbeeld via een digitale kopie.

2.4 Terugkoppeling



Een veelgehoorde opmerking van medewerkers is: *‘Ook al meld ik het, ik hoor toch niets meer terug.’* Tegelijkertijd geven leidinggevenden aan dat ze het vaak lastig vinden om terug te koppelen en goede nazorg te verlenen, omdat veel medewerkers slecht bereikbaar zijn door wisselende diensten en niet dagelijks aanwezig zijn. Er zijn een aantal momenten waarop medewerkers in ieder geval terugkoppeling moeten krijgen:

- Meteen na de melding, om aan te geven dat de melding is ontvangen;
- Zodra de melding bij de leidinggevende terecht is gekomen, om te checken hoe het met de medewerker is;
- Na inzet van de politie;
- Wanneer er op grond van de melding acties zijn ondernomen;

- Eén of twee keer per jaar, wanneer de cijfers van alle geregistreerde incidenten zijn geanalyseerd;
- Na het verhalen van schade;
- Bij of na een strafzaak bij justitie.

Ontvangst van de melding

Bij een melding via intranet kan de melder een digitale terugkoppeling krijgen. Degene die het formulier ontvangt dient de terugkoppeling te geven. Dat kan de leidinggevende zijn, maar ook de arbofunctionaris, de veiligheidscoach, de beveiligingsmedewerker die de gegevens in het incidentregistratiesysteem registreert, of een vertrouwenspersoon.

Aandacht voor de medewerker

Elke medewerker waardeert het wanneer zijn leidinggevende na een incident informeert hoe het met hem gaat. Bij incidenten met verbale agressie, dus zonder bedreigingen, is het misschien niet altijd nodig om een persoonlijke terugkoppeling te geven. Dat hangt af van de situatie waarin de verbale agressie zich voordeed. Was dat bijvoorbeeld 's nachts en was de medewerker alleen? Of ging het om agressie dat gerelateerd was aan een ziektebeeld? Dan kan de leidinggevende nagaan wat de aanleiding was en of de medewerker de situatie goed aankon. Er zijn ook medewerkers die geen behoefte hebben aan terugkoppeling. Dat moeten zij op het meldingsformulier kunnen aangegeven. Het blijft een taak van de leidinggevende om op medewerkers te letten. Zeker bij meerdere incidenten met dezelfde collega.

Inzet van politie

Als de politie betrokken is geweest bij een incident, of als er aangifte is gedaan, is het belangrijk om de jurist in de organisatie te laten vertellen wat er met de dader is gebeurd. Ook een terugkoppeling over een eventuele veroordeling van de dader is belangrijk. Het Openbaar Ministerie (OM) kan dit direct doen, maar ook een vaste contactpersoon van de organisatie bij de politie kan dit terugkoppelen. Heeft uw organisatie een eigen medewerker die de aangiftes bij de politie verzorgt, dan kan deze ook informeren bij het slachtofferloket van het OM. Wanneer (na een aangifte) het dossier van de verdachte bij het OM ligt, krijgt het slachtoffer zelf een terugkoppeling van het OM. Om als organisatie ook op de hoogte te blijven moet de organisatie zich in de aangifte als benadeelde partij laten opnemen. Dit werkt hetzelfde als bij het verhalen van schade.

In gang gezette acties

Het nabespreken van een incident kan leiden tot acties. Het belangrijk dat de medewerker van die acties op de hoogte wordt gesteld en gehouden. Medewerkers zien daardoor wat er met hun melding gebeurt, waardoor ze gestimuleerd worden om te blijven melden.

Vallen deze acties onder de verantwoordelijkheid van andere medewerkers, dan kunnen zij de stand van zaken komen toelichten. Als er een veiligheidscoach aanwezig is kan deze het proces bewaken. De veiligheidscoaches binnen de organisatie kunnen in een intern overleg de ervaringen delen en zo hun kennis samen verbreden. Daarmee worden incidenten voorkomen.

Analyse van geregistreerde incidenten

Door één of twee keer per jaar (bij veel incidenten ieder kwartaal) de geregistreerde incidenten te analyseren, kunt u de doelstellingen evalueren. Door de resultaten vervolgens met de medewerkers te bespreken, geeft u hen niet alleen waardering voor het feit dat ze hebben gemeld, maar ook inzicht in het effect van de genomen maatregelen. In hoofdstuk 2.7 en 2.8 gaan we hier verder op in.

- Erkenning voor de ervaring van de medewerker;
- Het bevorderen van collegiale steun;
- Het bevorderen van steun van de leidinggevende;
- Het bevorderen van de Safety en Security Awareness;
- Het bevorderen van kwaliteitstrainingen;
- Het bevorderen van eventueel herstel;
- Het bevorderen van het veiligheidsgevoel binnen het team;
- Preventieve maatregelen ontwikkelen;
- Tips verkrijgen van collega's.

Vormen van nabespreking

Een nabespreking kan verschillende vormen hebben. Met alleen de betrokken medewerker, met (een deel van) het team (bijvoorbeeld tijdens de overdracht na de dienst), tijdens het werkoverleg, of met alle betrokkenen tijdens een apart overleg. Het analyseren van het incident, waar we in 2.8 verder op ingaan, is iets anders. Dat is echt bedoeld om één of meer incidenten op een gestructureerde manier te analyseren, er uit te leren en met voorstellen voor verbetering te komen. Soms gebeurt dat voor een deel al tijdens de nabespreking. Dan lopen nabespreking en analyse in elkaar over, tijdens één bijeenkomst. In sommige organisaties worden alle incidenten consequent nabesproken, in andere organisaties gebeurt dat incidenteel of worden alleen de grotere incidenten nabesproken. Soms wordt het incident alleen door de beveiliging en de politie nabesproken, maar dat is te mager.

Knel- en verbeterpunten bij het nabespreken

De volgende knelpunten kunnen naar voren komen op het gebied van nabespreken:

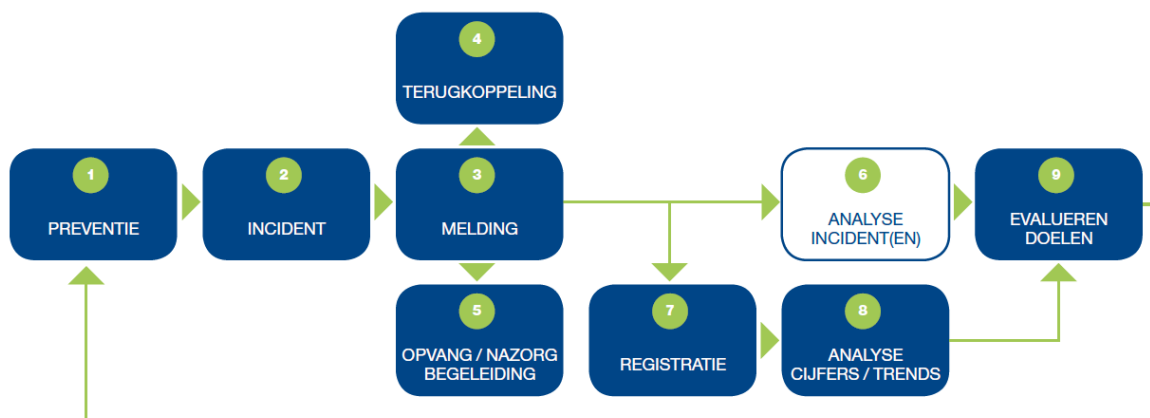
1. Medewerkers zijn er zich niet van bewust dat nabespreken zinvol kan zijn;
2. Veel agressie en geweld is ziektebeeld gerelateerd en dus niet te voorkomen. Daardoor hebben medewerkers het gevoel dat het geen zin heeft om na te bespreken;
3. Er zijn soms maar weinig incidenten;
4. Medewerkers verwachten van zichzelf en van hun collega's dat ze weerbaar zijn en om kunnen gaan met agressie
5. Of er wel of niet wordt nabesproken hangt erg af van de persoonlijkheid en de ervaringen van de teamleider;
6. Het kost veel tijd om medewerkers te bereiken. Soms zijn ze overdag niet altijd aanwezig;
7. Als een medewerker na een incident vrij is, kan het nabespreken erbij inschieten;
8. Het is soms lastig om iedereen bij elkaar te krijgen;
9. Vaak gebeurt het nabespreken niet door afwezigheid van de leidinggevende of de teamleider;
10. Tijdgebrek en werkdruk zorgen er vaak voor dat er niet wordt nabesproken;
11. Het kan moeilijk zijn om medisch specialisten bij een nabespreking te betrekken.

Om de knelpunten op te lossen kunt u de volgende verbetervoorstellen inzetten:

1. Spreek de leidinggevende aan op zijn verantwoordelijkheid;
2. De leidinggevende houdt in zijn agenda bij wanneer er met wie een nabespreking moet worden gehouden;
3. De veiligheidscoach houdt in de gaten of er ook echt een nabespreking is gehouden en monitort de registratie;
4. Alle betrokken disciplines worden bij de nabespreking betrokken, zodat de conclusies, afspraken en aanbevelingen meteen met iedereen gedeeld worden;
5. De nabespreking wordt een verplicht onderwerp op de agenda van het werkoverleg. De teamleider krijgt de verantwoordelijkheid om dit goed te organiseren;
6. Bespreek incidenten tijdens de overdracht aan het eind van de dienst;
7. De projectleider Veiligezorg@ kan in het begin aanschuiven bij de nabespreking, om het nut ervan aan te geven en om de teamleider enthousiast te maken;
8. Door beter te communiceren over het Bedrijfsopvangteam (BOT) creëert u meer bewustzijn;
9. U kunt de nabespreking institutionaliseren, zoals bij Veilig Incidenten Melden (bij patiënten);
10. Voer een goede methodiek in voor het nabespreken en analyseren van incidenten;
11. Zet een Bedrijfsopvangteam (BOT) op;
12. Neem het bespreken van incidenten op in het functieprofiel van de leidinggevende, de veiligheidscoach en de medewerker;

13. Neem een overzicht van alle incidenten (inclusief de gevolgen en kosten) op in het jaarverslag van de OR.

2.6 Analyse incident(en)



Het analyseren van een incident is niet hetzelfde als nabespreken. Nabespreken van een incident kan al door bij de overdracht van een dienst (of tijdens het eerstvolgende werkoverleg) te informeren hoe iemand het incident heeft ervaren en of iemand iets kwijt wil over het incident. Dit is meer gericht op de opvang en het verwerken van het gebeurde. Het analyseren van een incident gaat verder. Er wordt dan heel gedetailleerd gekeken wat er is gebeurd, welke afspraken er waren en wat er uit het incident geleerd kan worden. Een ander verschil is dat bij de nabespreking het accent ligt op de opvang van de betrokkene(n). Bij de analyse gaat het juist om het zoeken naar verbeteracties, om herhaling te voorkomen. De analyse vindt altijd met zoveel mogelijk van de betrokkenen plaats, bijvoorbeeld tijdens het teamoverleg. Daarbij kunnen meerdere vergelijkbare incidenten tegelijk worden geanalyseerd.

Tijdens de analyse wordt ieder incident systematisch en gestructureerd besproken. Dat kan alleen als medewerkers goed zijn opgevangen en elkaar op gedrag kunnen aanspreken. Belangrijk is dat melders van incidenten niet als schuldige wordt aangewezen en dat reacties worden voorkomen als: 'gek hè, het overkomt altijd jou!'. Zo'n sfeer zorgt ervoor dat medewerkers daarna geen incidenten meer durven te melden en er ook niet meer over willen praten. Bij de analyse kijken betrokkenen naar de mogelijke aanleiding en naar de omstandigheden waaronder het incident is ontstaan of geëscaleerd. Daarbij staan ze ook stil bij de afspraken die in het verleden zijn gemaakt om agressie te voorkomen. Vervolgens formuleren ze actiepunten, of passen oude afspraken aan.

Waarom analyseren?

Door incidenten na te bespreken en te analyseren stelt u medewerkers in staat om op het werk te praten over hun ervaringen en daar samen van te leren. Alleen wanneer u incidenten regelmatig analyseert, kunt u nagaan of de gemaakte afspraken en verbeteringen ook echt leiden tot minder agressie, het beter omgaan met agressie en een veiliger gevoel bij de medewerkers. Juist als de organisatie open en vrij is over agressie-incidenten, zullen medewerkers hier ook open over spreken.

Het analyseren van incidenten heeft in ieder geval de volgende doelen:

- Het verkennen van knelpunten, oorzaken en oplossingen;
- Het ontwikkelen van een verbetercultuur;
- Het werken aan een veilige sfeer op de afdeling en in de organisatie.

Wanneer analyseren?

Incidenten met een grote impact, zoals het gebruik van fysieke agressie, (ernstige) bedreigingen, het gebruik van verboden wapens of de inzet van politie, moeten altijd binnen een week worden nabesproken en geanalyseerd. Leidinggevenden zijn hiervoor verantwoordelijk. Bij de rest van de incidenten is het voldoende om deze een of twee keer per jaar te analyseren, afhankelijk van de mate waarin de incidenten voorkomen. Tijdens de analyse kunt u stilstaan bij één specifiek

incident, bij een representatief voorbeeld, of bij een aantal vergelijkbare incidenten op de afdeling. U kunt ook incidenten bespreken die op een andere afdeling zijn gebeurd, maar op de eigen afdeling hadden kunnen plaatsvinden.

Hoe analyseren?

Het analyseren van incidenten kan het beste gestructureerd gebeuren. Zo voorkomt u dat bepaalde zaken niet aan bod komen. Ook is het belangrijk dat er medewerkers bij zijn die bij het incident aanwezig waren. Tijdens de analyse kijkt u niet alleen naar de omstandigheden die tot het incident hebben geleid, maar ook naar de manier waarop alle betrokkenen met het incident zijn omgegaan. De betrokkenen staan stil bij de aanleiding van het incident, de opvang, de begeleiding en de nazorg tijdens en na het incident, de contacten met de beveiliging en eventuele externe partners (zoals politie en justitie), alle procedures en andere afspraken, de melding en de terugkoppeling.

Belangrijke voorwaarden om samen incidenten te kunnen analyseren zijn:

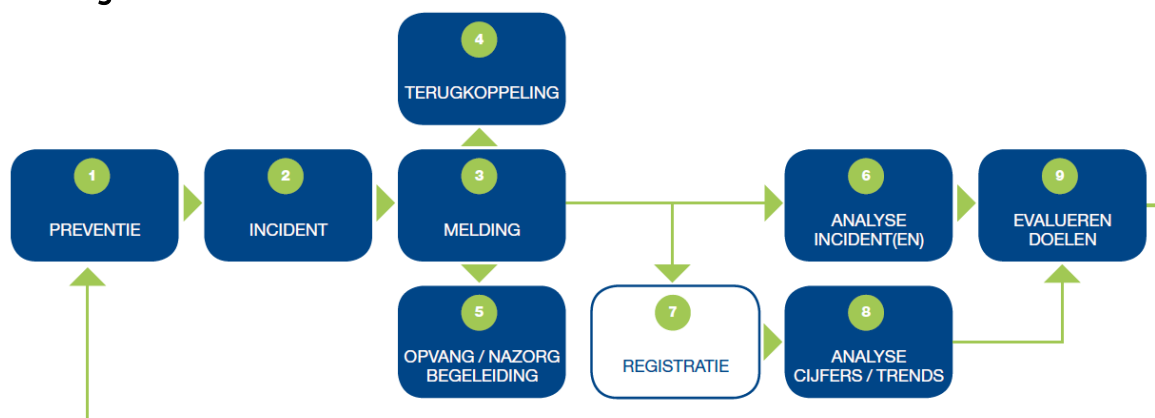
- 'Blame free' melden. Medewerkers moeten zich uitgenodigd voelen om incidenten te melden, zonder dat ze een stempel opgedrukt krijgen. Daar passen geen verwijten of beschuldigingen bij, maar een positief kritische houding, gericht op verbeteringen;
- Erkenning van het gebeurde;
- Een goede eerste opvang. De ervaring leert dat wanneer opvang en nazorg ontbreken, de getroffen medewerkers zich niet goed begeleid voelen. Daardoor stellen zij zich bij het onderzoeken van de oorzaken terughoudend op;
- Het lijnmanagement moet verantwoordelijk zijn voor opvang, begeleiding en nazorg en voor het scheppen van verbetervoorwaarden;
- Een bottom-up benadering. Medewerkers zijn tijdens het analyseren de ervaringsdeskundigen, omdat zij hun eigen werksituatie het beste kennen;
- De gespreksstof blijft vertrouwelijk en wordt niet onnodig buiten het overleg verspreid.

Wie leidt de bespreking?

Meestal begeleidt de teamleider of het hoofd van de afdeling de bijeenkomst. Dit kan echter ook de veiligheidscoach, een getrainde medewerker, een maatschappelijk werker of een vertrouwenspersoon zijn. De belangrijkste taken van degene die de bijeenkomst leidt zijn:

- Een sfeer van vertrouwen creëren, waarin medewerkers zich uitgenodigd voelen om vrijuit te spreken;
- Goed luisteren;
- De structuur van het overleg in de gaten houden, zodat alle punten besproken worden;
- De tijd bewaken;
- Het gesprek samenvatten;
- Afsluiten met concrete actiepunten;
- Zo nodig taken verdelen, inclusief een tijdsplan.

2.7 Registratie



Wanneer er een incident is geweest, dan is het de bedoeling dat medewerkers dat melden. Zoals we al in hoofdstuk 2.3 hebben beschreven, geven medewerkers met een melding een aantal gegevens over het incident door.

Vervolgens worden de ontvangen gegevens gecontroleerd, aangevuld, geregistreerd en gemonitord en worden eventuele acties ondernomen.

Waarom registreren?

Registreren is nodig om:

- Doelen te evalueren en het evaluatieproces te onderbouwen;
- Prioriteiten te kunnen stellen op basis van feiten en cijfers;
- Begrotingsvoorstellen te kunnen onderbouwen met feiten en cijfers;
- De voortgang van nazorg en begeleiding te bewaken;
- De voortgang in het ketenproces te bewaken;
- Goed en duidelijk te kunnen communiceren op basis van feiten;
- Safety en Security Awareness te creëren;
- Ziekte-dagen, verhaalde schade en de inzet van het BOT te monitoren.

Een van de voornaamste redenen om te registreren, is om er achter te komen hoeveel incidenten er zijn geweest in een bepaalde periode. Eén van de doelstellingen is immers minder incidenten. Om dat te kunnen bepalen heeft u cijfers nodig. Wanneer uw doelstellingen SMART zijn geformuleerd, zijn ze ook meetbaar. In dat geval kunt u met de cijfers uit het registratiesysteem kijken of uw doelstellingen worden bereikt. De gegevens die u registreert, hebben dus alles te maken met de doelen die u heeft gesteld en de vragen waarop u antwoord wilt hebben. Dat antwoord leidt vervolgens tot oplossingen om de mate van agressie en het aantal incidenten te verminderen.

U kunt op basis van de gegevens uit het registratiesysteem ook prioriteiten stellen ten aanzien van de inzet van de beveiliging; hoe meer incidenten op een bepaald tijdstip of een bepaalde locatie, hoe meer beveiliging u in kunt zetten op die momenten en op die plekken. Bij de afhandeling van een incident kunnen ook ketenpartners als de politie, justitie en de gemeente betrokken zijn. In het incidentregistratiesysteem kunt u hierover informatie opnemen. Dat maakt het mogelijk om de afhandeling van waarschuwingen, toegangsontzeggingen en aangiften te bewaken.

Wat registreren?

U moet in ieder geval de volgende gegevens registreren:

- Een uniek nummer;
- De gegevens van het slachtoffer;
- Het type slachtoffer (medewerker, patiënt, bezoeker, artsassistent, medisch specialist, verpleegkundige, externe medewerker, stagiaire, patiëntbegeleider, student);
- De functie van het slachtoffer;
- De veroorzaker (persoonsgegevens en type);
- Eventuele getuige(n) (persoonsgegevens en type);
- Het type incident (geweld, schade/diefstal, ordeverstoring, gevaarlijke situatie, bommelding, etc.);
- De locatie (maak gebruik van de kamernummering);
- De datum en het tijdstip;
- De afdeling;
- De aanleiding;
- Het soort geweld;
- De gevolgen van het incident;
- De eventuele betrokkenheid van politie of ketenpartners;
- De maatregelen die zijn genomen door de organisatie;

Voorbeelden van vragen:

1. Wat voor type incidenten komen er voor?
2. Waar komen de incidenten voor?
3. Waar komen ze vaker voor?
4. Wie zijn de slachtoffers?
5. Wie zijn de veroorzakers?
6. Wanneer komen de incidenten voor?
7. Op welke tijdstippen en op welke dagen in de week?
8. Wanneer komen ze vaker voor?
9. Waardoor ontstaan incidenten?
10. Wat is de aanleiding?
11. Komen bepaalde incidenten meer voor dan andere?
12. Wat gebeurt er?
13. Is er letsel toegebracht?
14. Zijn er voorwerpen bij betrokken?
15. Zijn de gevolgde trainingen effectief?
16. Welke incidenten zijn ziektebeeld gerelateerd?
17. Zijn er trends te bespeuren?

- officiële waarschuwing;
- officiële toegangszegging;
- stoppen van de dienstverlening;
- schadeverhaal;
- aangifte;
- Eventueel (ziekte)verzuim van slachtoffer(s) en medewerker(s);
- De voortgang monitoren en eventueel bijsturen.

Hoe registreren?

Er bestaan verschillende systemen en programma's om de gegevens in te registreren. Welk systeem u gebruikt is eigenlijk niet zo belangrijk, zolang u maar die gegevens registreert die nodig zijn om de vragen over uw doelstellingen en uw beleid te kunnen beantwoorden.

Wie registreert er?

Het registreren (de invoer van de gegevens) gebeurt meestal door een medewerker van de beveiliging of door een arbo-adviseur. Aangezien de leidinggevende van de afdeling verantwoordelijk is voor de medewerkersveiligheid op de afdeling, is het logisch dat de leidinggevende zelf registreert of dat dit namens hem wordt gedaan door de veiligheidscoach op de afdeling. Juist doordat er binnen de organisatie een beperkt aantal mensen mag registreren, is de privacy gewaarborgd. Anderen krijgen geen toegang tot het systeem. Verder is het zo dat deze personen het systeem goed leren kennen, weten wat er gevraagd wordt en bekend zijn met het doel van het registreren. Het invullen vergt daardoor minder tijd. Als iedere medewerker zelf moet registreren mist de organisatie een goede kans om aandacht te schenken aan zowel de medewerker als aan het incident. Aangezien medewerkers veelal niet thuis zijn in het systeem, vergt het hen ook veel meer tijd.

Het gebruik van de gegevens

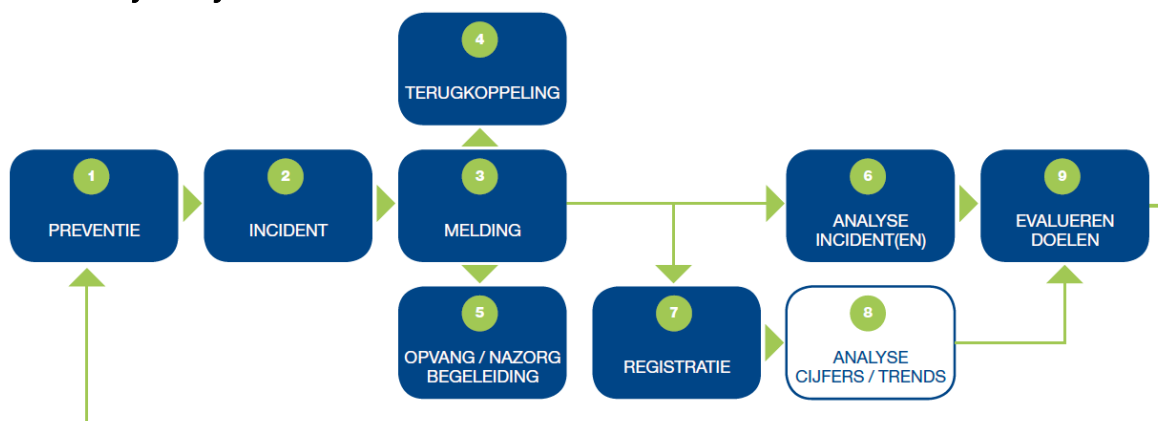
Een goed opgezet registratiesysteem levert behalve cijfers ook informatie over de afhandeling van de incidenten, bijvoorbeeld over de aangifte, een eventuele veroordeling van de veroorzaker, waarschuwingen en toegangszeggingen. Zorg ervoor dat de medewerkers (de melders) hier ook iets over terug horen. Als u medewerkers van dit soort zaken op de hoogte brengt, motiveert dat hen om te blijven melden.

Soms worden meldingsformulieren niet volledig ingevuld. In feite is dit alleen een probleem wanneer de leidinggevende (of degene die dit voor de leidinggevende doet) geen kans ziet om contact te leggen met de melder/het slachtoffer.

TIP

Soms ontstaat er een achterstand bij het registreren (door werkdruk of andere oorzaken). Lukt het niet om gegevens over incidenten consequent en structureel in te voeren? Kan de taak verdeeld worden? Of is er wellicht iemand die terugkomt van een ziekteproces en dit zou kunnen doen?

2.8 Analyse cijfers en trends



Een analyse van de geregistreerde cijfers kan veel informatie opleveren voor het maken, evalueren en aanpassen van beleid. Het koppelen van de verschillende gegevens in het registratiesysteem levert u vaak nog meer informatie op.

Wie doet de analyses?

Degene die verantwoordelijk is voor het maken van de rapportages is ook degene die analyses maakt. Vaak is dat een arbo-adviseur of een hoofd beveiliging. Op afdelingsniveau is dat de leidinggevende. Stel voordat u aan de analyse begint de vraag: Wat willen we weten? Wat is de doelstelling van de registratie? Bij het formuleren van de vragen, het analyseren van de rapportages en het maken van verbetervoorstellen kan de veiligheidscoach een belangrijke rol vervullen. Denk hierbij ook aan het overleg tussen de veiligheidscoaches. Neem de ervaringen uit dit overleg mee in de jaarrapportage, de RI&E en het MTO.

Aanpassen van het beleid

U kunt de cijfers gebruiken om het beleid op verschillende niveaus te evalueren en aan te passen: op afdelings- en clusterniveau (als onderwerp van overleg met de leidinggevende), op centraal niveau ter motivatie van het beleid, op afdelingsniveau in het arbo-jaarverslag en op het niveau van de RvB, het MT en de OR.

Een analyse van de cijfers kan op diverse onderwerpen inzicht opleveren. Hieronder leest u een aantal voorbeelden.

1. Inzet beveiliging

- Op welke momenten komen de incidenten voor?
- Moet dat leiden tot een andere inzet van de beveiliging?
- Is de samenwerking met de ketenpartners politie, gemeente en OM in orde, of dient deze te worden bijgesteld?

2. Training

- Welk type incident komt er op een bepaalde afdeling, of bij een bepaalde groep, meer voor?
- Moet daar in een training aandacht aan worden besteed?
- Is het trainingsbureau de juiste partner voor de geconstateerde problematiek?

3. Opvang en nazorg

- Welke groep medewerkers heeft meer opvang en aandacht nodig, omdat deze met meer of ernstigere incidenten te maken heeft?
- Welke groep medewerkers is sneller emotioneel geraakt en heeft misschien meer opvang en nazorg nodig?

4. Preventie

- Zijn er afdelingen waar meer aan preventie moet worden gedaan omdat er meer incidenten voorkomen?
- Kan er gericht beleid richting de veroorzakers van agressie worden gevoerd op basis van hun kenmerken?
- Kan er gericht aan preventie worden gedaan op grond van de oorzaken of aanleiding van incidenten?

5. Evaluatie beleid

- Wat is het beleid bij verbale agressie, bedreigingen of fysieke agressie? Houden medewerkers zich daar aan?
- Is het gevoel van veiligheid verbeterd door het veiligheidsbeleid?

6. Kosten

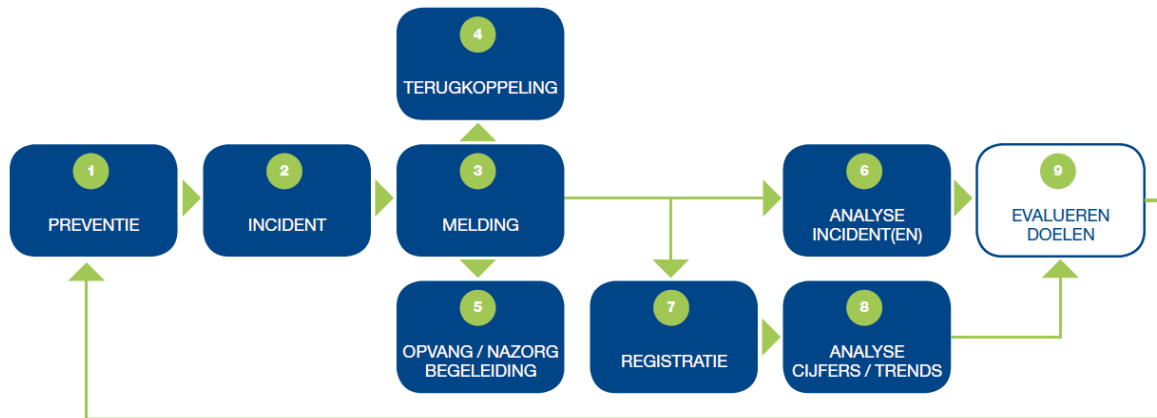
- Wat waren de kosten van letsel, schade en verzuim?
- Wat kan er verhaald worden en wat is verhaald? (Denk hierbij ook aan de relatief lage kosten. Daarmee toont u medewerkers dat bepaald gedrag niet getolereerd hoeft te worden)
- Wat waren de kosten van de extra inzet van diverse medewerkers?

Terugkoppeling

Door één of twee keer per jaar de resultaten uit de rapportages en de analyses te bespreken, houdt u medewerkers gemotiveerd. Zij zien hierdoor wat hun melding oplevert, welke maatregelen er zijn

genomen en wat het effect hiervan is. Koppel de jaarlijkse cijfers en analyses ook terug naar de OR en de Raad van Bestuur, zodat zij inzicht krijgen in het effect van de investeringen.

2.9 Evalueren doelen



Zoals u in deze handreiking al een paar keer heeft gelezen, is het evalueren van doelen onmogelijk zonder cijfers. Meten is weten. Zelfs een kwalitatieve doelstelling als ‘medewerkers voelen zich veiliger’, dient u kwantitatief te formuleren. Het doel wordt dan bijvoorbeeld: ‘20 procent meer medewerkers voelen zich veilig’.

Ook kunt u het veiligheidsgevoel zelf kwantificeren met een cijfer. De kern van de zaak is: zonder doelen te stellen kunt u niet gericht aan de aanpak van agressie werken en zal nooit duidelijk worden of alle inzet en geld effect hebben.

Heeft u nog vragen? Stuur uw vraag naar veiligezorg@caop.nl



Deze handreiking is in opdracht van AO VVT en VeiligeZorg en de sociale partners

