HOFFMANN TIPS

voor bedrijfsleven en publieke sector

#238 | oktober 2019

- *Toch herkenbaar 'in beeld' bij diefstal*
- *Hardnekkige roddels*
- *CEO-firewall*
- *Organisaties moeten waakzaam blijven en met de tijd meegaan"*
  - audit Port of Amsterdam

Hoffmann

Column

The usual suspects

In ons werk krijgen wij veel te maken met de *usual suspects*: de directeur, de financieel manager en de medewerker met veel vrijheid, op wie weinig tot geen toezicht is. Verhoudingsgewijs doen we veel onderzoek naar leidinggevenden. En dat is complex! Vaak is een leidinggevende namelijk nog gewoon werkzaam voor een organisatie als ons onderzoek start. Het is dan belangrijk dat we ons onderzoek snel, maar ook op een discrete manier uitvoeren.

In één van de casussen in deze Hoffmann Tips leest u over een frauderende schooldirecteur. Hoe kan het gebeuren dat een leidinggevende jarenlang zijn gang kan gaan, vraagt u zich dan misschien af. *"Ik vond het al gek"* of *"Ik heb het weleens aangekaart, maar daar werd niets mee gedaan"* zijn helaas uitspraken die we regelmatig horen tijdens ons onderzoek. Best gek, als u het mij vraagt. Blijkbaar zijn de onregelmatigheden dus meestal wel bekend. Of heeft men op zijn minst een onderbuikgevoel dat er iets niet klopt. Hoe zorgt u binnen uw organisatie voor een cultuur waar dit soort signalen naar boven komen? En hoe gaat uw organisatie op een juiste manier met dit soort signalen om? In het artikel op pagina 3 leest u hoe integriteitsgesprekken u kunnen helpen om het integriteitsbeleid (verder) vorm te geven.

Leidinggevenden blijken aan de ene kant vaak de pleger van fraude te zijn. Aan de andere kant zijn ze ook vaak het doelwit van fraude. Denk aan de CEO-fraude waar we nog steeds over horen in het nieuws en over lezen in de krant. Het risico op dit soort fraude is reëel. Zeker als uw organisatie internationaal georiënteerd is en een hiërarchische structuur heeft. Wat kunt u als organisatie doen om zich tegen deze vormen van CEO-fraude te wapenen? We delen een aantal ideeën in de artikelen over de audit op het betaalproces (pagina 4) en over de weerbaarheid van uw organisatie (pagina 8).

Als Hoffmann zijn we heel goed in het achteraf oplossen van een incident, bijvoorbeeld door (digitaal) forensisch onderzoek te doen. Maar ik vind het juist ook heel interessant om samen met u, onze klant, te bespreken hoe u uw organisatie weerbaar kunt maken om incidenten in de toekomst te voorkomen. Want voorkomen blijft toch altijd beter dan genezen. Ik hoop dat de artikelen in deze Hoffmann Tips u weer verder aan het denken zetten.

Veel leesplezier!

MARTIJN VAN DE BEEK

Integriteitsgesprekken: een thermometer in uw organisatie

Integriteit is voor iedere organisatie belangrijk. Als er binnen een organisatie normen worden overschreden, dan kan dat niet alleen negatieve gevolgen hebben voor de werksfeer, maar ook voor het imago en - uiteindelijk - de omzet. Toch weet niet iedere directie hoe medewerkers omgaan met integriteitsvraagstukken. In die gevallen kan Hoffmann met integriteitsgesprekken een thermometer in de organisatie steken.

Waarom integriteitsgesprekken?
Wanneer u als directie niet precies weet hoe uw medewerkers met integriteitsvraagstukken omgaan, dan kunnen daar verschillende oorzaken voor zijn. Een snelle periode van groei bijvoorbeeld, waardoor de prioriteiten even elders lagen, of verouderd integriteitsbeleid. Maar ook personeelsverloop of vervanging van een voltallig bestuur kunnen oorzaken zijn. Om grip te krijgen op het integriteitsbeleid kan het dan goed zijn om een onafhankelijke derde partij in te schakelen om te onderzoeken hoe de organisatie ervoor staat, om van daaruit het integriteitsbeleid (weer) verder vorm te kunnen geven.

Onze aanpak: maatwerk
Hoffmann voert individuele gesprekken met een dwarsdoorsnede van de organisatie: directie, administratie, HR-managers en uitvoerende medewerkers van alle afdelingen en alle locaties. De onderwerpen die daarbij aan bod komen worden altijd afgestemd met en op de organisatie. De hiernavolgende thema's komen in ieder geval aan bod:

Beleid
Heeft de organisatie integriteitsbeleid? Weten medewerkers dit beleid te vinden? Weten zij bij wie incidenten gemeld moeten worden? Is er een vertrouwenspersoon? Is hij of zij toegankelijk?

Leiderschap
Maken leidinggevenden integriteit bespreekbaar? Vertonen zij voorbeeldgedrag?

Seksuele intimidatie
Komt dit voor op de werkvloer? Of in digitale communicatiemiddelen (zoals WhatsApp-groepen)? Weet men hoe om te gaan met grensoverschrijdend gedrag? En wordt ertegen opgetreden?

Corruptie, omkoping, diefstal en fraude
Worden medewerkers wel eens in de verleiding gebracht? Hoe gaan zij hiermee om? Weten zij eigenlijk wat er wel en niet mag?

Vervolgens ontvangt de organisatie een rapportage met onze bevindingen en handvatten om het integriteitsbeleid verder vorm te geven.

Veiligheid en vertrouwen
Om te zorgen dat de te interviewen medewerkers zich veilig voelen om informatie te delen, verzamelt Hoffmann tijdens de gesprekken geen persoonsgegevens. Ook zorgen wij ervoor dat in de rapportage opgenomen incidenten niet tot personen herleidbaar zijn.

Casus

Toch herkenbaar 'in beeld' bij diefstal

Meerdere keren waren er 's nachts dure spullen gestolen uit het magazijn van een groothandel in de metaalindustrie. De dieven beschikken over sleutels om het bedrijfsterrein op te komen en het magazijn te openen. Betrokkenheid van één van de medewerkers lijkt waarschijnlijk. Vooral ook omdat de dieven precies weten waar ze moeten zijn en heel gericht te werk gaan. De diefstallen zijn op camera vastgelegd, maar ... de dieven weten duidelijk waar de camera's hangen. Ze komen niet herkenbaar in beeld. Daarom schakelt de directeur ons in om onderzoek te doen.

Onderzoek via een andere invalshoek
De daders zijn op de camerabeelden onherkenbaar. Daarom kiezen we in het onderzoek een andere invalshoek: via digitaal forensisch onderzoek kijken we of het WiFi-netwerk van het bedrijf meer kan vertellen over de dieven. Wat blijkt? Op het moment dat de dieven het terrein opreden, maakte een (zakelijke)smartphone verbinding met het WiFi-netwerk van het bedrijf. Toen de dieven vertrokken, werd ook de verbinding met het WiFi-netwerk verbroken. Bij nader onderzoek konden we achterhalen welke medewerker deze smartphone gebruikt had.

Confrontatie met de dader
Twee van onze onderzoekers gaan het gesprek aan met de verdachte medewerker. Hij bekent al snel dat hij de diefstallen heeft gepleegd en de spullen heeft doorverkocht. Dit resulteerde in een ontslag.

Door het snelle handelen na de laatste diefstal kwam de doorbraak in dit digitale onderzoek. Doordat de loggegevens nog beschikbaar waren leidde dit tot de dader.

Bij diefstal, fraude of een cyberincident laat een betrokken medewerker vaak digitale sporen achter. Zorg ervoor dat die digitale sporen ook bruikbaar zijn voor onderzoek. Wilt u weten of uw organisatie goed genoeg voorbereid is op digitaal forensisch onderzoek? Onze Forensic Readiness Scan geeft u antwoord op die vraag.

Audit op het betaalproces

Factuurfraude en CEO-fraude: voor oplichters lucratieve business. Aan organisaties de taak om scherp en alert te blijven.

Frauderisico's in het betaalproces
In rechercheonderzoeken naar factuur- en CEO-fraude zien wij vaak dat betalingsprocessen van organisaties niet 100% waterdicht zijn. Zo constateren wij regelmatig dat beleid en/of procesbeschrijvingen ontbreken, procesbeschrijvingen onvolledig of verouderd zijn, de uitvoering in de praktijk afwijkt van de proces-beschrijvingen en er onvoldoende functiescheiding is gerealiseerd.

Op het moment dat zo'n fraude wordt ontdekt en Hoffmann voor het onderzoek wordt ingeschakeld is de schade vaak al geleden. De organisatie kan dan alleen nog maatregelen nemen om herhaling in de toekomst te voorkomen. Een typisch geval van 'Als het kalf verdronken is dempt men de put.'

Organisaties die dat voor willen zijn, kunnen een audit op het betaalproces laten uitvoeren. De auditors van Hoffmann hebben ruime ervaring met het onderzoeken van factuur- en CEO-fraude. Daardoor weten zij als geen ander waar zij op moeten letten. Tijdens de audit beoordelen zij de aanwezige procesbeschrijvingen, interviewen zij alle medewerkers die een rol spelen in het betaalproces en controleren zij de systemen. Vervolgens ontvangt de organisatie een heldere rapportage met kwetsbaarheden en aanbevelingen.

Casus: Port of Amsterdam
Port of Amsterdam is verantwoordelijk voor het scheep-vaartverkeer in het gebied van het Noordzeekanaal, de infrastructuur en verhuur van grond binnen het havengebied en het innen van havengeld. Alexander Kousbroek, Finance Director en Head of Finance and Control bij Port of Amsterdam, woonde in 2018 een kennissessie van Hoffmann over factuur- en CEO-fraude bij. Daarop vroeg hij Hoffmann om een audit op het betaalproces uit te voeren.

Tijdens de audit bleek dat het betaalproces bij Port of Amsterdam goed in elkaar zit. Hoffmann heeft geconstateerd dat de processen goed zijn beschreven, de risico's doorlopend worden geïdentificeerd en dat er een goede functiescheiding is, zowel bij medewerkers als in het systeem. Bovendien doen de medewerkers wat er van hen wordt verwacht. Dit betekent dat risico's op factuurfraude en CEO-fraude bij Port of Amsterdam laag zijn. Mocht er toch iets gebeuren, dan is de kans groot dat de fraude snel wordt ontdekt.

Lees op de volgende pagina de ervaring van Alexander Kousbroek.

"Organisaties moeten waakzaam blijven en met de tijd meegaan."

"Toen ik in 2015, na 9 jaar bij Deloitte in de auditpraktijk te hebben gewerkt, bij Port of Amsterdam startte, was het een van mijn opdrachten om de financiële basisprocessen op orde te brengen, deze processen te beschrijven en ze toetsbaar te maken. Ik wilde de processen zo inrichten dat het niet onmogelijk werd om betalingen te doen: het moest wel werkbaar blijven. Maar daardoor blijf je wel risico's houden.

Tijdens de kennissessie van Hoffmann viel het mij op hoe geraffineerd fraudeurs te werk gaan. Ik was benieuwd hoe ons proces en de maatregelen die wij op dat moment hadden geïmplementeerd door Hoffmann werden beoordeeld. Daarnaast wilde ik weten of wij nog zaken konden aanscherpen.

Ik ben tevreden over de professionele uitvoering van de audit. De samenwerking verliep heel soepel, terwijl Hoffmann echt kritisch naar ons betaalproces heeft gekeken. Natuurlijk ben ik blij dat de beoordeling zo positief was. Onze afdeling is zich heel erg bewust van de verschillende risico's en dat wordt door deze audit bevestigd. Maar uiteraard blijven we ook na deze audit de interne beheersing verbeteren. Dat is een continu proces. Als organisatie moet je altijd waakzaam blijven en met de tijd meegaan."

Alexander Kousbroek
Finance Director/Head of Finance and Control Port of Amsterdam

Column

Continuïteit

Continuïteit is essentieel voor elk bedrijf en overheidsinstelling. Niet alleen voor de eigen gemoedsrust, maar voornamelijk in het belang van de klant die geen verstoring wenst van bedrijfsprocessen. Risicomanagement en kennis van de processen van de eigen onderneming zijn dan ook een must in het moderne zakendoen.

Met stijgende verbazing heb ik van de zijlijn het 112 crisis-incident bij KPN geobserveerd. Het eerste wat in mij opkwam was volslagen paniek, geen coördinatie en totaal onvoorbereide noodhulpdiensten.

Het tweede wat mij opviel was de directe aanval op KPN als de schuldige. Nu moet gezegd: KPN heeft wel een probleempje. Meerdere back-up systemen welke niet werken op het moment suprême. Een software bug wordt gezegd. Dit kan gebeuren. Zo werd Royal Bank of Scotland (RBS) een aantal jaren geleden getroffen door een software bug. Als gevolg hiervan werkte de back-up systemen niet waardoor de klanten in het Verenigd Koninkrijk meer dan een week geen overboekingen kon doen. Waarom ik de link naar een bank maak? RBS had een Business continuity en Crisismanagement Plan.

U moet weten dat de overheden in Europa en dus ook in Nederland, via wet- en regelgeving hebben vastgelegd dat instellingen die deel uitmaken van de zogenaamde kritische infrastructuur, uitgebreide business continuity plannen en crisismanagement protocollen moeten ontwikkelen, implementeren, trainen en testen. Eén van de uitgangspunten is dat je wel processen, maar verantwoordelijkheden niet kunt uitbesteden. En daar ligt dan ook tegelijkertijd de ruimte voor adviezen over risicomanagement voor Hoffmann.

In het geval van het 112-incident is pijnlijk vast komen te staan dat de overheid kennelijk niet gecontroleerd heeft of de back-up systemen van KPN in een simulatie werkten. Nog erger, en bijna grenzend aan voorwaardelijke opzet, moet er op basis van de huidige informatie worden geconcludeerd dat de noodhulpdiensten kennelijk geen plan hadden klaarliggen voor dit incident. Wat het allemaal nog erger maakt is dat het allemaal al eens eerder heeft plaatsgevonden. Men heeft niet geleerd.

Als dit bij een bank zou gebeuren, dan was de toezichthouder, De Nederlandsche Bank, naar alle waarschijnlijkheid een groot onderzoek gestart en zouden de verantwoordelijken moeten vrezen voor hun baan. Of erger: De Nederlandse Bank zou de instelling onder curatele stellen.

Een overheid die regels oplegt aan bedrijven, maar zelf niet de discipline heeft om die regels zelf na te leven, die overheid faalt. Het past die overheid ook niet direct naar de externe partij te wijzen. In dit geval KPN. Die overheid bleef gedurende het incident verantwoordelijk voor noodhulpdienstverlening. Die verantwoordelijkheid kan die overheid nooit afschuiven.

Niet alle klanten van Hoffmann behoren tot de kritische infrastructuur van Nederland. Maar zij hebben wel een zorgplicht jegens hun klanten. Een oplossing zou kunnen zijn een assessment te doen van kritische processen. Hebben de klanten van Hoffmann een incidentmanagement plan klaarliggen? Ik ben bang van niet. En als dat klopt dan vind ik dat kwalijk. Voor de gemoedsrust van de bedrijven, maar nog meer voor hun klanten. Ik ga een stapje verder, iedereen neemt kennis van de gebeurtenissen bij KPN, doet een plas en alles blijft zoals het was. Net als de overheid na het eerste 112 incident.

Fred Teeven
Directeur Verinq BV Risicomanagement

verinq

Een frauderende schooldirecteur

Een factuur voor nieuwe winterbanden voor de schoolauto valt een medewerker van een scholengemeenschap op. Want de bedrijfsauto rijdt niet met nieuwe banden rond. Maar de auto van de directeur wel! Als de medewerker melding maakt van dit geval, wordt deze melding niet serieus in onderzoek genomen. Het is dan 2017. Ruim een jaar later: een televisiescherm blijkt ineens verdwenen te zijn. Als de medewerker de camerabeelden bekijkt, ziet hij de directeur met het televisiescherm weglopen. Hij deelt zijn zorgen met een hogergeplaatste medewerker. Die onderneemt actie en stapt uiteindelijk naar de Raad van Bestuur.

De kluis met bijna een ton aan contanten

De Raad van Bestuur gaat begin van dit jaar in gesprek met de schooldirecteur en stelt hem tijdelijk op non-actief. De schooldirecteur ontkent geld van de school voor privédoeleinden te hebben gebruikt. Hij zou het geld hebben overgemaakt naar privé en vervolgens gepind hebben om minder belasting te hoeven betalen. Hij wijst de Raad van Bestuur op een kluis waarin bijna een ton aan contant geld ligt. De Raad van Bestuur vraagt aan ons om een onderzoek in te stellen.

Administratief en digitaal onderzoek

Wij analyseren de bankrekeningen van de school én de privérekeningen van de schooldirecteur (uiteraard met zijn toestemming). Ook analyseren we alle uitgaven en kunnen zo een tijdlijn maken. Uit ons onderzoek blijkt dat de directeur wel degelijk geld heeft weggesluisd naar privérekeningen van hemzelf en gezinsleden. Een paar dagen na het gesprek met de Raad van Bestuur blijkt de schooldirecteur met een plastic tas onder de arm de kluisruimte te betreden. Dat blijkt uit camerabeelden van de school. Later bekent de schooldirecteur dat hij op dat moment bijna een ton aan contanten in de kluis heeft gelegd. Mogelijk wilde hij doen voorkomen dat het totale geldbedrag van de schoolrekening (al die tijd al) in de kluis lag, omdat hij verwachtte ontmaskerd te worden.

Ontslag en een rechtszaak

De schooldirecteur wordt door onze rechercheurs met de feiten geconfronteerd. Hij heeft de kans om zijn kant van het verhaal te vertellen. De Raad van Bestuur besluit de frauderende schooldirecteur op basis van de resultaten uit ons onderzoek op staande voet te ontslaan. Niet terecht volgens de directeur. Hij is wel fout geweest, maar wilde het geld alleen aan de school besteden, beweert zijn advocaat. De schooldirecteur vecht het ontslag aan bij de rechtbank. In juli van dit jaar oordeelt de rechter dat de schooldirecteur terecht op staande voet is ontslagen. De Raad van Bestuur hoeft de schooldirecteur geen schadevergoeding te betalen en vordert ook het verdwenen geld terug.

Als een medewerker een melding doet over (financiële) onregelmatigheden, neem dat dan altijd serieus. In deze casus waren de onregelmatigheden al veel eerder opgevallen, maar kreeg de oplettende medewerker in eerste instantie geen gehoor bij leidinggevenden. Iets waar deze leidinggevenden later ook op aangesproken zijn.

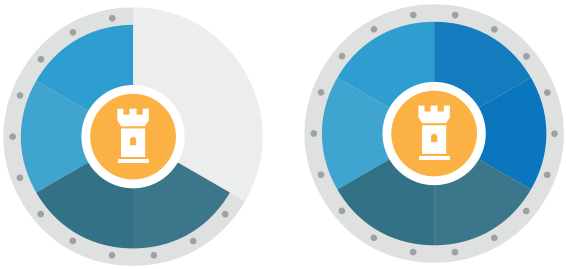
Hoe weerbaar is uw organisatie tegen CEO-fraude?

CEO-fraude, een misleidende term. Veelal wordt met behulp van social engineering een medewerker in de organisatie beïnvloed om een financiële transactie te verrichten of een rekeningnummer aan te passen. Het is dus niet de CEO die fraudeert, maar het lijkt alsof de CEO telefonisch of per mail een opdracht geeft om een dergelijke transactie uit te voeren. Hierbij wordt vaak zeer zorgvuldig te werk gegaan, te denken valt aan vervalste (digitale) handtekeningen of een gespooft telefoonnummer. Recentelijk was zelfs in het nieuws dat een bedrijf was opgelicht door een telefoontje met een stem die klonk als de stem van de CEO (BNR[1]). Om tegen dergelijke aanvallen weerstand te bieden is technisch veel mogelijk, maar uiteindelijk gaat het erom hoe de medewerker handelt. De kwetsbaarheid zit dus voor een groot deel ín de eigen organisatie.

Een analyse van deze vorm van fraudegevallen geeft inzicht in de kenmerken van organisaties die kwetsbaar zijn voor CEO-fraude: Bedrijven die o.a. internationaal georiënteerd zijn, hiërarchisch en met de beslisbevoegdheid hoog in de organisatie zijn vaker slachtoffer (Weijkamp & Van Esch, 2019). Het betreffen veelal eigenschappen die hun oorsprong hebben in de bedrijfscultuur. Het is dus zinvol om na te gaan hoe je als organisatie scoort op deze kenmerken. De CEO-firewall brengt overzichtelijk in kaart waar kwetsbaarheden zitten en waar de organisatie goed beschermd is (zie figuur 1).

Door het op structurele wijze in kaart brengen van de kwetsbaarheden kunnen er gerichte interventies worden ingezet om de organisatie weerbaarder te maken. Dit betreffen maatwerkoplossingen op het gebied van de organisatie, de techniek én de mens. Met specifieke doelgroepen, zoals bijvoorbeeld het directieteam of de financiële administratie, wordt door ons team psychologen concreet gemaakt wat het gewenste gedrag is en middels interviews onderzocht waarom dit niet (altijd) optreedt. Een voorbeeld van dit gedrag is dat men extra controles uitvoert wanneer er gevraagd wordt buiten de vastgelegde procedures te handelen, bijv. in een e-mail. Dit klinkt eenvoudig, maar wanneer er veel druk op de medewerker wordt gelegd, zien we dat dit regelmatig mis gaat. Op basis van de interviews worden interventies geformuleerd, die concreet en toepasbaar zijn. Het resultaat van het cultuurveranderingstraject is een zogenoemde sterke CEO-firewall: een organisatie die weerbaar is tegen CEO-fraude. Lees meer op www.hoffmann.nl[2].

De CEO firewall



Figuur 1. De CEO-firewall voor een kwetsbare en een beschermde organisatie, op basis van kenmerken van de bedrijfscultuur

[1] https://www.bnr.nl/nieuws/technologie/10388515/oplichters-gebruiken-nu-de-stem-van-je-baas
[2] https://hoffmann.nl/fraude-integriteit/voorkomen-incidenten/ceo-firewall

Red Teaming internationaal

Ons team van specialisten voert wereldwijd Red Teaming testen uit. Deze testen omvatten een combinatie van zowel de fysieke als de digitale veiligheid van organisaties. Onderdelen hiervan zijn bijvoorbeeld openbronnenonderzoek, gerichte penetratietesten, spearfishing, voicephishing en fysieke inloop. Middels een aanvalssimulatie worden kwetsbaarheden (en tevens sterke kanten) van de geteste organisatie in kaart gebracht. Het team kruipt in de huid van mogelijke kwaadwillende actoren, om zo realistisch mogelijk via verschillende scenario's organisaties te testen. Deze scenario's worden uitgebreid besproken en afgestemd met de opdrachtgever. Hierbij is tevens nadrukkelijk aandacht voor de wettelijke kaders van het betreffende land waarbinnen geopereerd wordt en staat volledige debriefing van de medewerkers centraal.

Organisaties hebben vaak al veel maatregelen getroffen om zich weerbaar(der) te maken tegen dergelijke aanvallen. Aan de hand van de testen kan beoordeeld worden of de reeds opgezette veiligheidsmaatregelen voldoende werken en of er op veiligheidsgebied mogelijk nog zaken missen. Er worden aan de hand van de bevindingen vervolgens aanbevelingen gedaan op het gebied van organisatie, techniek én de mens.

Hardnekkige roddels

Wat doet u als twee medewerkers elkaar tegenspreken bij een ernstige beschuldiging? Die vraag houdt één van onze opdrachtgevers in de energiebranche bezig. Eén van de betere onderhoudsmonteurs wordt beschuldigd van drugsgebruik tijdens het werk. Verschillende collega's uiten deze beschuldiging, maar de onderhoudsmonteur blijft stellig ontkennen. Wat moet hij doen om zijn onschuld te bewijzen? De directie vraagt ons om mee te denken over een oplossing. En de onderhoudsmonteur geeft aan dat hij graag wil meewerken om zijn onschuld te bewijzen.

Steekproef door een drugsswap

De onderhoudsmonteur is altijd onderweg en werkt op verschillende locaties. Geen vaste werkplek dus die we kunnen onderzoeken. Wel gebruikt de onderhoudsmonteur elke dag zijn bestelbus. Volgens de beschuldigingen van zijn collega's bewaart hij de drugs in het dashboardkastje en gebruikt hij de drugs ook in de bestelbus. Onze medewerkers besluiten een drugsswap te doen op verschillende plekken in de bestelbus. Een laagdrempelige manier om vast te stellen of er inderdaad drugs gebruikt zijn op die plek. Op een dag verschijnen we onverwacht op de werklocatie van de onderhoudsmonteur. Ook onze opdrachtgever is aanwezig bij de tests die we doen. Het resultaat? Er is niets te vinden.

Bewijs ontkracht de roddels

De opdrachtgever gaat vervolgens het gesprek aan met de collega die de roddels heeft verspreid. Wat blijkt? In het verleden is er onenigheid geweest tussen de onderhoudsmonteur en zijn collega. Geen reden natuurlijk om serieuze beschuldigingen zonder bewijs te verspreiden. Daar krijgt de collega dan ook een fikse waarschuwing voor. De opdrachtgever is blij dat hij de aanklacht heeft laten onderzoeken. Daarmee kreeg hij namelijk bewijs in handen om de hardnekkige roddels te ontkrachten.

ONDERZOEK NAAR **ZWART** VERZUIM

Het ziekteverzuim in Nederland kost werkgevers jaarlijks € 11,7 miljard aan loondoorbetalingskosten. Een werkgever die twijfelt of een werknemer daadwerkelijk arbeidsongeschikt is, kan dit laten onderzoeken. In dit artikel zullen wij ingaan op de wettelijke kaders waarbinnen een werkgever bij een onderzoek naar mogelijk zwart verzuim moet opereren.

Op grond van artikel 7:629 lid 1 BW behoudt een werknemer gedurende twee jaar recht op loon, indien hij zijn werk niet heeft verricht door ziekte. De werkgever heeft in verband met deze verplichting het recht om te (laten) controleren of de werknemer ziek/arbeidsongeschikt is en recht heeft op loon. Op grond van artikel 7:629 lid 3 BW heeft de werknemer geen recht op loon wanneer hij, hoewel hij daartoe wel in staat is, zonder deugdelijke grond passende arbeid niet verricht of wanneer hij weigert mee te werken aan door de werkgever gegeven redelijke voorschriften of getroffen maatregelen die erop gericht zijn om de werknemer in staat te stellen passende arbeid te verrichten.

De verzuimcontrole is de verantwoordelijkheid van de werkgever. Het is echter niet aan de werkgever om te oordelen over de arbeidsongeschiktheid van een werknemer. Een werkgever is namelijk (evenals een werknemer) leek op dit gebied. Wanneer de werkgever twijfels heeft over de arbeidsongeschiktheid dient de werkgever zich tot de bedrijfsarts te wenden, waarna de bedrijfsarts zijn oordeel over de arbeidsongeschiktheid kan geven. Eventueel kunnen de werkgever en de werknemer vervolgens een second opinion aanvragen bij het UWV.

Een bedrijfsarts kan beoordelen in hoever de klachten leiden tot arbeidsongeschiktheid. Ook kan een bedrijfsarts beoordelen waartoe een zieke werknemer gezien zijn klachten of beperkingen nog in staat is (passende arbeid). Van de zieke werknemer wordt dan ook verwacht dat hij de bedrijfsarts van de nodige, juiste informatie voorziet in verband met het beoordelen van de arbeidsongeschiktheid (en daarmee recht op loon) en de re-integratie.

Wanneer een werknemer zich ziek veinst, wordt dit zwart verzuim genoemd. Zwart verzuim is een vorm van fraude. De werkgever die een werknemer wegens zwart verzuim op staande voet wil ontslaan, zal dan onomstotelijk moeten bewijzen dat de werknemer niet arbeidsongeschikt is. Het kan dan raadzaam zijn een recherchebureau in te schakelen, maar voorzichtigheid is geboden.

De rechter toetst het inschakelen van een recherchebureau aan de eisen van goed werkgeverschap. Er moet een concreet vermoeden van fraude bestaan en de werkgever moet op basis van feiten en omstandigheden redelijkerwijs hebben kunnen overgaan tot het instellen van een onderzoek. Het doen controleren van een

werknemer buiten zijn medeweten door een recherchebureau is slechts aanvaardbaar 'onder zeer bijzondere omstandigheden waarin tegen de werknemer ernstige verdenkingen zijn gerezen ter zake van ernstige overtredingen, welke een onderzoek buiten de betrokkene om noodzakelijk maken'. Het inschakelen van een recherchebureau om ziekte te controleren is alleen toelaatbaar 'indien er voldoende objectieve en genoegzame redenen zijn voor het maken van een inbreuk op het privéleven van de werknemer'. Indien vervolgens uit de bevindingen van het recherchebureau blijkt dat de werknemer zich schuldig maakt aan zwart verzuim, is ook voorzichtigheid geboden. Dit blijkt uit een recente uitspraak van de kantonrechter Rotterdam.

De casus: werknemer is sinds 15 april 2017 in dienst van werkgever, in de functie van Leerling Operationeel Medewerker. Op 10 december 2018 is werknemer tijdens het werk in zijn nek geraakt door een container, als gevolg waarvan hij is gevallen. Werknemer heeft zich na dit ongeval ziek gemeld. Begin februari 2019 heeft werkgever aan een recherchebureau de opdracht gegeven te onderzoeken of werknemer activiteiten ontplooide die strijdig waren met het door hem opgegeven ziektebeeld. Uit onderzoek is onder meer gebleken dat werknemer tijdens ziekteverzuim bij herhaling handelingen verricht die strijdig zijn met het door hem opgegeven ziektebeeld. Bij brief d.d. 15 maart 2019 heeft werkgever werknemer op staande voet ontslagen. Werknemer vecht het ontslag op staande voet aan.

Volgens de kantonrechter blijkt uit de bevindingen van het recherchebureau dat werknemer, in ieder geval fysiek, (veel) meer mogelijkheden had dan hij zelf heeft aangegeven.

Door het recherchebureau is onder andere vastgesteld dat werknemer zonder fysieke beperkingen diverse huishoudelijke handelingen verricht (vuilniszak tillen, auto wassen), diverse keren zelf een auto bestuurt en meermalen intensief en langdurig traint in de sportschool. Het staat, aldus de kantonrechter, dan ook vast dat werknemer niet de waarheid heeft gesproken tegenover werkgever en de bedrijfsarts. Echter, werkgever had volgens de kantonrechter voorafgaand aan de inschakeling van het recherchebureau, maar in ieder geval na de eerste bevindingen van het recherchebureau, werknemer schriftelijk moeten waarschuwen en/of een deskundigenoordeel moeten aanvragen bij UWV met betrekking tot de vraag of en zo ja in hoever werknemer arbeidsongeschikt was en of hij voldoende meewerkte aan zijn re-integratie. Daarna had werkgever eventueel kunnen overgaan tot een loonstop en indien dat geen effect zou hebben, een ontbindingsverzoek bij de kantonrechter kunnen indienen. Omdat werkgever dit niet heeft gedaan, oordeelt de kantonrechter dat werkgever te snel gegrepen naar het middel van ontslag op staande voet. Bij dit oordeel kan overigens een vraagteken worden geplaatst, omdat werknemer niet is ontslagen wegens het schenden van re-integratie-verplichtingen, maar wegens het verstrekken van leugenachtige verklaringen over arbeidsongeschiktheid.

Resumé: indien u twijfelt of een werknemer daadwerkelijk arbeidsongeschikt is, laat u dan adviseren over een onderzoek en daarna eventueel een ontslag, zodat u de juiste stappen doet op de juiste momenten.

Mr. F.H.A. ter Huurne is advocaat en partner bij Lexence te Amsterdam (www.lexence.com)

Lexence advocaten & notarissen

Hoffmann

Vertrouwen is goed,

Hoffmann is beter

Over Hoffmann
Uw veiligheid, daar maken we ons sterk voor, al meer dan 57 jaar. Oplossingsgericht als het moet, dankzij onze doorgewinterde onderzoekers en adviseurs. Integer, objectief en altijd direct beschikbaar. Hoffmann bestaat uit twee afdelingen: Fraude & Integriteit en Cybersecurity & Security Risk Management.

Fraude & Integriteit
Een veilige werkomgeving voor u en uw medewerkers. Het lijkt een onbesproken arbeidsvoorwaarde. Helaas is de realiteit soms anders. Fraude, vernieling, diefstal, ongewenste intimiteiten, pesten; niemand wil dat, maar het gebeurt. In die gevallen rekent u direct op ons. Discreet, objectief en ervaren. Want na ruim 57 jaar durven we ons gerust specialist in fraude en integriteitsschendingen te noemen. Van deskresearch en observatie tot gespekken met betrokkenen.
Wij geven u de handvatten om juridisch sterker te staan. Met de garantie dat uw bedrijfsvoering daar zo min mogelijk hinder van ondervindt. Maar veel liever nog minimaliseren we de risico's die u, uw bedrijf of uw medewerkers lopen. Hoffmann heeft alles in huis om samen met u de route naar een veilige bedrijfscultuur in kaart te brengen én die te realiseren.

Cybersecurity & Security Risk Management
Een veilige bedrijfscultuur begint bij uzelf. Dat betekent niet dat u deze helemaal zélf hoeft te realiseren. Onze adviseurs en trainers werken samen met u én uw medewerkers aan een veilige werkomgeving. Samen met u richten ze veilige processen en effectieve controles in, en ze helpen u toewerken naar een veilige en integere cultuur.
Ons uitgangspunt is: veiligheid zie je niet, die voel je. De risico's met betrekking tot bedrijfscontinuïteit bevatten tegenwoordig vaak een digitale component. Wanneer er een incident plaatsvindt moet er snel geschakeld worden. Hoffmann biedt u dankzij onze scans, trainingen en praktische adviezen direct en adequaat het hoofd. Met de zekerheid dat uw bedrijf of organisatie ondertussen blijft functioneren en presteren.
Samen met u streven we naar een open bedrijfscultuur waar collega's elkaar durven aan te spreken, waar controle een vanzelfsprekend en positief karakter heeft en waar veiligheid ieders verantwoordelijkheid is. Een omgeving waar het risico op fraude en digitale incidenten tot een minimum beperkt is.

Bezoekadres: Luidsprekerstraat 10, 1322 AX ALMERE
Postadres: Postbus 60090, 1320 AB ALMERE
Telefoon: 088 - 298 6600
info@hoffmann.nl - www.hoffmann.nl