

HOFFMANN TIPS

voor bedrijfsleven en publieke sector

#239 | april 2020



De impact van
onverwachte
gebeurtenissen

- *Hoffmann en KPN Security beklinden samenwerking*
- *Workshop Digitaal Forensisch Onderzoek*
- *5 tips voor bedrijven in tijden van corona*
- *Lokmiddelen oplossing tegen diefstal*



Hoffmann

De impact van onverwachte gebeurtenissen



In de afgelopen weken zijn we met z'n allen in de ban van het coronavirus. De maatregelen worden alsmaar ingrijpender. En natuurlijk heeft dat ook invloed op uw organisatie. Zo werken bijvoorbeeld steeds meer medewerkers vanuit huis. Welke risico's brengt dat met zich mee en hoe gaat u daar als organisatie mee om? Helaas proberen cybercriminelen misbruik te maken van de thuiswerkmaatregelen. Daarom mag een artikel met vijf tips rondom thuiswerken wat ons betreft niet ontbreken. Houd rekening met de cyberrisico's die er in deze situatie ontstaan.

Toch gaan we het in deze Hoffmann Tips niet alleen hebben over de impact van het coronavirus. We kunnen het onderwerp namelijk breder trekken: er zijn meer onverwachte gebeurtenissen waarmee u als bedrijf te maken kunt krijgen. Bij Hoffmann komen we regelmatig in organisaties waar zich zo'n onverwachte gebeurtenis heeft voorgedaan. Onder andere als we onderzoek doen naar fraude of integriteitsschending. Steeds vaker horen we na afloop dat het onderzoek goed bevallen is, maar dat er daarna wel veel onrust in de organisatie is geweest. Niet zozeer onrust door het onderzoek zelf. Nee, eerder door het feit dat er blijkaar onderzoek nodig was.

Het is heel logisch dat medewerkers onrust en onveiligheid ervaren op de werkvloer na een onderzoek. Stelt u zich namelijk maar eens voor dat één van uw collega's op staande voet wordt ontslagen. De collega die altijd in was voor een praatje. Met wie u in de jarenlange samenwerking leuke herinneringen heeft opgebouwd. De collega bij wie u zelfs op kraambezoek geweest bent toen zijn jongste drie jaar geleden geboren werd. En nu? Nu hoort u dat hij gefraudeerd heeft. Logisch dat het vertrouwen van medewerkers dan een deuk oploopt. Maar wat doe je daaraan?

Het zat ons niet lekker dat er na ons onderzoek nog zoveel onrust kan ontstaan op de werkvloer. Want een veilige werkomgeving? Daar maken we ons al meer dan 57 hard voor! Onderzoek naar fraude of identiteitsschending kan een enorme impact hebben op de samenwerking binnen een bedrijf. Het is goed om die impact te herkennen en te erkennen. Daarom zijn we sinds kort een samenwerking aangegaan met een gecertificeerde psycholoog naar wie we kunnen doorverwijzen. Deze psycholoog faciliteert de interne gesprekken na een onderzoek. Hoe gaan u en uw medewerkers om met het onderzoek dat is geweest? Wat speelt er bij de medewerkers? En hoe kan het eventueel beschadigde onderlinge vertrouwen weer hersteld worden?

Dit is een voorbeeld van hoe we ons netwerk steeds uitbreiden om u nog beter te kunnen helpen. In het artikel op pagina 3 leest u meer over onze samenwerking met de psycholoog voor nazorg bij fraude en identiteitsschending. En ook het artikel op pagina 6 gaat over een nieuwe samenwerking. Maar natuurlijk vindt u ook nog andere casussen en artikelen in deze Hoffmann Tips. Ook over het voorkomen van incidenten. Zoals op pagina 7 de tips voor thuiswerkers tijdens de maatregelen rondom het coronavirus.

Ik hoop dat deze informatie u helpt nu uw organisatie met een onverwachte gebeurtenis wordt geconfronteerd!

MARTIJN VAN DE BEEK

Fraude en integriteitsschending vraagt soms om nazorg

Hoffmann houdt zich al bijna 60 jaar bezig met fraude- en integriteitsonderzoeken binnen bedrijven. Ondanks de grote zorgvuldigheid en de discretie waarmee wij werken zien wij dat die onderzoeken soms best wel een grote impact kunnen hebben. Niet alleen op de betrokkene(n) zelf, maar ook op de rest van de organisatie.

Impact verschilt

Hoe medewerkers reageren op een fraudeonderzoek hangt uiteraard af van de uitkomsten van dat onderzoek, maar ook van de cultuur binnen een organisatie én van de individuele medewerkers. In de meeste gevallen zien wij dat medewerkers al vrij snel weer overgaan tot de orde van de dag.

Maar soms blijven medewerkers achter met veel emoties: boosheid, verdriet en onzekerheid. Vaak hebben zij dan ook veel vragen. Het was zo'n fijne collega. We missen hem toch. Hoe heeft dit kunnen gebeuren? Zullen ze denken dat ik er ook bij betrokken was? Worden we vanaf nu allemaal in de gaten gehouden? Kortom, soms is het vertrouwen binnen een team of afdeling na een fraudeonderzoek sterk verminderd, en duurt het even voordat medewerkers de draad echt weer op kunnen pakken.

Ook leidinggevenden kunnen na een fraudeonderzoek met vragen blijven zitten. Wat betekent dit voor de effectiviteit van mijn team? Voor de processen? En hoe herstel ik het (gevoel van) vertrouwen? Zij kunnen dan behoefte hebben aan een ervaren klankbord om mee te sparren.

Samenwerking met een psycholoog NIP

Vanuit de gedachte dat wij onze klanten ook op dit vlak nazorg willen verlenen is Hoffmann een samenwerking gestart met een ervaren psycholoog NIP. Deze samenwerking geeft onze klanten de mogelijkheid om haar al tijdens of na het onderzoek in te schakelen voor de begeleiding van hun medewerkers.

Onze partner is een zelfstandig gevestigd psycholoog, organisatieadviseur en coach. Haar doel is mensen te ondersteunen om (weer) meer grip te krijgen op werksituaties. Zij heeft veel ervaring met het begeleiden van teams die onder grote druk, wijzigingen of veranderingen, effectief samen moeten werken.

Zij werkt al een aantal jaar samen met Hoffmann en kent het team van onderzoekers en hun werkwijze goed. Dat maakt dat zij haar inzet bij onze klanten efficiënt en effectief kan aansluiten op de dienstverlening van Hoffmann.

Klanten van Hoffmann kunnen haar, via Hoffmann, inschakelen voor onafhankelijk advies aan leidinggevenden, ondersteuning van individuele medewerkers en teambegeleiding.

Factuur voor nooit ontvangen bedrijfskleding

Niemand weet de bedrijfskleding te vinden, maar de facturen zijn wel betaald. Zelfs al vóór de leverdatum. Daarbij is opvallend dat de facturen niet van de reguliere leverancier zijn. De boekhouder speurt verder ... Wat blijkt? De medewerker die de bedrijfskleding besteld zou hebben, heeft ook 50.000 euro overgemaakt naar zijn privérekening. Een bedrag dat hij later weer in delen terugstort. Genoeg alarmbellen voor deze overheidsinstantie om ons te vragen om onderzoek te doen.

Stap 1: onderzoek in de boekhouding

Allereerst analyseren we de boekhouding nauwkeurig. De facturen voor de bedrijfskleding blijken niet volgens het gewone proces in de boekhouding te zijn gekomen. Ook zien we dat de betreffende medewerker de facturen heeft ingediend en als enige heeft geaccordeerd. Raar, want normaal accorderen minimaal twee personen de facturen binnen deze organisatie. Als derde valt op dat de factuurnummering niet klopt.

Stap 2: onderzoek in open bronnen

Heeft de leverancier de boel misschien opgelicht? We besluiten een openbronnenonderzoek te doen. Daaruit blijkt dat deze leverancier de broer van de medewerker is. Dit duidt op belangverstrengeling! De opdrachtgever

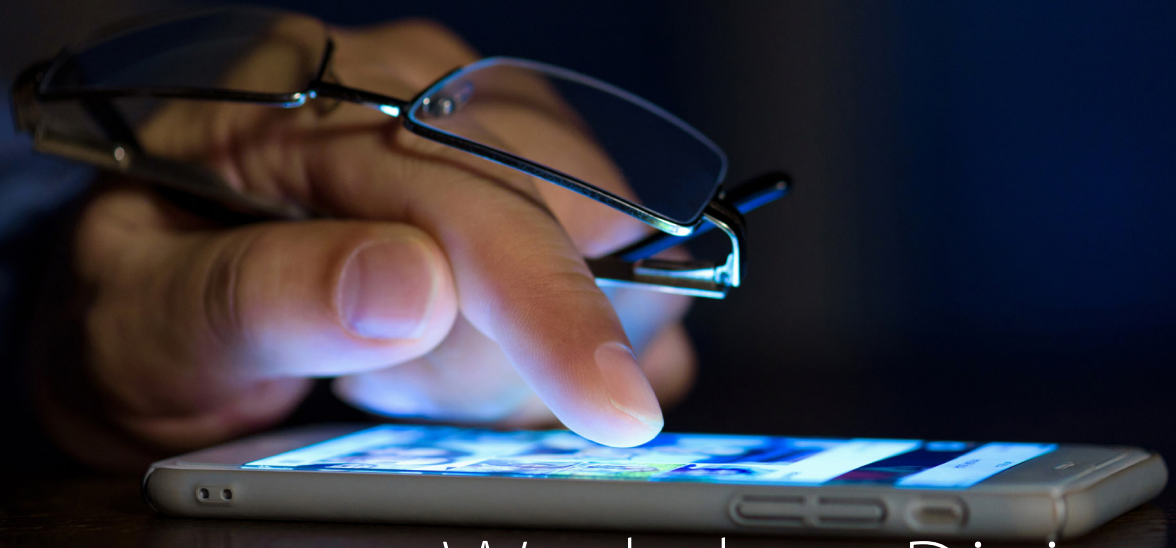
stelt de medewerker voorlopig op non-actief. Ook vraagt de opdrachtgever ons om verder onderzoek te doen.

Stap 3: digitaal onderzoek

We onderzoeken de computers en telefoons van de medewerker. Daar vinden we diverse aanwijzingen dat er iets niet klopt. Onder andere een mail met de opmerking 'kijken of ze deze factuur opmerken bij de boekhouding'. Daarnaast valt een patroon op: steeds als er een factuur voor bedrijfskleding werd betaald, betaalde de medewerker via zijn eigen rekening een deel van de 50.000 euro terug aan de overheidsinstantie. Het wordt helemaal duidelijk als onze onderzoekers een sms vinden van de medewerker aan zijn broer. Daarin staat dat hij met de opbrengst van de facturen een privéschuld kan aflossen.

De afloop van ons onderzoek

Tijd voor een confrontatie met de feiten. De overkomsten tussen de bedragen op de facturen, op zijn rekening en in de sms kan de medewerker niet verklaren. Uiteindelijk bekent hij schuld. Aangifte en ontslag volgen. Ook doet de overheidsinstantie aangifte tegen de broer van de medewerker.



Workshop Digitaal Forensisch Onderzoek, eerstelijnscontrole

Sinds 1 november 2019 is het strafbaar om bepaalde voorwerpen, waaronder gegevensdragers en communicatiemiddelen, binnen te brengen in een justitiële inrichting. Daarnaast moeten justitiabelen die gebruik mogen maken van een (spel)computer, laptop of mobiele telefoon zich aan strenge regels houden. Om medewerkers van justitiële inrichtingen te leren hoe zij een controle kunnen uitvoeren op digitale voorwerpen, ontwikkelde Hoffmann de workshop 'Digitaal Forensisch Onderzoek, eerstelijnscontrole'.

Opzet workshop

De workshop duurt 5 uur, is geschikt voor maximaal 15 deelnemers en bestaat uit een theoretisch gedeelte en een praktijkgedeelte. Tijdens het theoretisch gedeelte wordt onder meer aandacht besteed aan de mogelijkheden om bestanden en informatie te verbergen, de verschillende bestandstypen en bestandsformaten, encryptie en de laatste stand van de techniek.

Het praktijkgedeelte vormt het grootste gedeelte van de workshop. In dit gedeelte gaan de deelnemers aan de slag met een controleopdracht. Daarbij moeten zij binnen een bepaalde tijd een controle uitvoeren op verschillende door Hoffmann geprepareerde gegevensdragers en communicatiemiddelen, zoals spelcomputers, laptops, horloges en mobiele telefoons. Na afloop van deze opdracht mogen de deelnemers hun bevindingen aan elkaar presenteren.

Doel workshop

Het doel van deze workshop is om de medewerkers die belast zijn met de eerstelijnscontrole kennis en bewustzijn bij te brengen over de do's en don'ts bij een controle. Zij krijgen praktische handvatten mee om een controle zo veilig en effectief mogelijk uit te voeren. Ook leren zij wanneer zij een specialist moeten inschakelen.

De Van der Hoevenkliniek

De Van der Hoevenkliniek is een forensische zorginstelling met meerdere locaties. Op de locatie Utrecht worden voornamelijk patiënten behandeld die een tbs-maatregel opgelegd hebben gekregen. In 2019 volgden 30 medewerkers de workshop 'Digitaal Forensisch Onderzoek, eerstelijnscontrole'. Silvia Verwoerd, plaatsvervangend hoofd van de inrichting en adviseur van de raad van bestuur, en Michel Hartman, ambulante sociotherapeut, vertellen er meer over.





“We willen graag dat de medewerkers die de controles uitvoeren een hoog kennisniveau hebben en precies weten wanneer ze moeten stoppen met zelf controleren.”

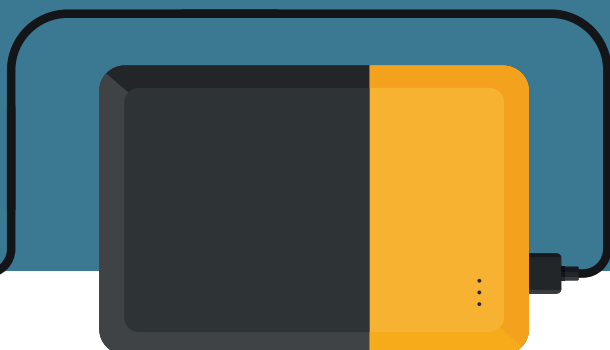
“Veel van onze patiënten wonen transmuraal en hebben de beschikking over spelcomputers, zoals een Xbox of een PlayStation”, vertelt Michel. “Daarnaast bereiden we patiënten in de laatste fase van hun behandeling voor op een terugkeer in de maatschappij. Dat betekent dat zij ook moeten oefenen met het gebruik van internet, laptops en een telefoon. Omdat er onder onze patiënten ook hoogrisicopatiënten zijn, willen we goed zicht houden op hun datadragers. We controleren ze dan ook regelmatig. Daarbij hangt het van het risicoprofiel van de patiënt af hoe vaak we dat doen.”

“We willen graag dat de medewerkers die de controles uitvoeren een hoog kennisniveau hebben en precies weten wanneer ze moeten stoppen met zelf controleren”, vervolgt Silvia. “Sommige van onze patiënten zijn technisch geschoold en dus heel erg handig. Daarom hebben 30 van onze medewerkers de workshop van Hoffmann gevolgd.” Michel: “De ontwikkelingen op technisch gebied gaan zo snel. Apparaten krijgen steeds meer mogelijkheden en worden steeds toegankelijker. Neem een PlayStation, daar kan je bijna net zo veel mee als met een gewone computer.”

Op de vraag wat hij van de opzet van de workshop vond, antwoordt Michel: “Het is goed dat eerst de theorie wordt behandeld. Juist omdat de technische ontwikkelingen zo snel gaan, is het belangrijk bij te blijven. Bovendien hebben we een aantal goede tips meegekregen voor ons beleid. Zo hebben we op een mobiele telefoon van sommige patiënten ouderlijk toezicht ingesteld zodat we zicht hebben op wat voor apps patiënten installeren.”

“De praktijkoefeningen sluiten heel goed aan bij onze dagelijkse praktijk”, vervolgt Michel. Ze zijn leuk en nuttig. En het is fijn dat je ook met apparatuur kunt oefenen waar je niet dagelijks mee te maken hebt. Daardoor kom je weer op scherp te staan. Bovendien leer je in deze workshop precies wanneer je moet stoppen en de zaak moet overdragen aan een forensisch specialist. En ik ben een liefhebber, maar eigenlijk had ik nog meer willen oefenen. De workshop had van mij dus langer mogen duren.”

*Silvia Verwoerd, plaatsvervangend hoofd van de inrichting en adviseur van de raad van bestuur
Michel Hartman, sociotherapeut binnen een transmuraal team*





Hoffmann en KPN Security beklinken samenwerking

Overeenkomst ondertekend tijdens evenement NLSecure[ID]

Hoffmann en KPN Security intensiveren de onderlinge samenwerking. Martijn van de Beek (directeur Hoffmann) en Marcel van Oirschot (Executive Vice President KPN Security) plaatsten beiden hun handtekening onder de samenwerkingsovereenkomst.

GGI Veilig-programma

KPN is met meer dan 130 jaar ervaring een begrip in ondernemend Nederland en biedt samen met KPN Security een volledig securityportfolio en bijbehorende dienstverlening om private en publieke organisaties te helpen in de groei naar digitale weerbaarheid. Mede door die positie is KPN Security de grote winnaar van de GGI Veilig-aanbesteding en actief op alle drie de percelen.

Naast dat KPN zijn eigen REDteam met ethical hackers heeft, wordt binnen GGI Veilig samengewerkt met Hoffmann. Die samenwerking heeft onder andere betrekking op het uitvoeren van pentesten en forensisch onderzoek. KPN Security consultancy helpt de risico's in kaart te brengen en zo stap voor stap de digitale weerbaarheid van bedrijven te vergroten en vervolgens een securitybeleid te ontwikkelen van reactief naar risico gebaseerd.

Bewezen in het publieke domein

“Wij hebben gekeken welke partij ons op dit gebied het beste kan ondersteunen”, zegt Van Oirschot. “Hoffmann heeft een uitstekende reputatie en kent de gemeentemarkt en de bijbehorende stakeholders. De uitkomsten van een pentest of forensisch onderzoek kunnen tevens terechtkomen bij burgemeesters en wethouders, de Rekenkamer, of de burgers. De juiste verwoording, conclusies en aanbevelingen en een discrete manier van werken zijn dan van cruciaal belang. Hoffmann kent dit speelveld en heeft zich bewezen in het publieke domein.”

“De inzet van Hoffmann voor pentesten borgt daarnaast ook een zuivere balans tussen de inrichting van de securityomgeving en de toetsing op deze inrichting. Ook bij levering van diensten uit perceel 1 en 2 door KPN wordt door deze samenwerking een objectieve toetsing gewaarborgd”, aldus Van Oirschot.

Martijn van de Beek: “In KPN Security consultancy vinden wij de ideale partner, met een zelfde visie op cybersecurity en cyberweerbaarheid en met veel kennis en ervaring in deze specifieke markt. Vanuit Hoffmann kunnen wij met onze pentesten kwetsbaarheden zichtbaar maken in systemen, in processen en bij de mensen die hiermee werken, waar KPN vervolgens meteen concreet toepasbare oplossingen kan bieden. Door deze samenwerking ontstaat een ijzersterke combinatie.”

5 tips voor bedrijven in tijden van corona

Het coronavirus is een ongekende crisis, die de wereld in zijn greep heeft en voorlopig nog niet voorbij is. Uiteraard is eenieders gezondheid eerste prioriteit. Daarnaast moeten bedrijven oog houden voor de (digitale) veiligheid. In dit artikel geeft Hoffmann daarvoor 5 tips.

Tip #1 Wijs uw medewerkers op de gevaren van phishing

Nu veel medewerkers thuiswerken, zien cybercriminelen hun kans schoon om wachtwoorden en gebruikersnamen buit te maken en netwerken binnen te dringen. Het aantal phishingberichten (valse e-mails en voicephising) is de afgelopen periode verveelvoudigd.

Wij adviseren u daarom uw medewerkers op deze gevaren te wijzen. Vraag ze hun gezond verstand te gebruiken: kennen zij de afzender van een e-mailbericht niet? Dan doen ze er verstandig aan om niet op een link te klikken. Spreek ook met ze af om in een inkomend telefoongesprek nooit inloggegevens en persoonlijke en/of vertrouwelijke informatie te verstrekken. Laat ze in plaats daarvan vragen of ze op een later moment kunnen terugbellen.

Tip #2 Zorg voor veilige verbindingen en werkprocessen

Veel van de coronamaatregelen die op 16 maart zijn genomen kwamen vrij onverwacht. Voor veel bedrijven was de eerste prioriteit dan ook om zo veel mogelijk operationeel te blijven en het personeel aan het werk te houden. Dat betekent dat er in allerlei thuiswerkverbindingen zijn opgetuigd, waarbij veel medewerkers via hun eigen Wifi-verbinding en op hun eigen apparatuur aan het werk zijn gegaan. Dat brengt risico's met zich mee.

Nu de eerste storm enigszins is gaan liggen, adviseren wij u om zo snel mogelijk voor veilige verbindingen (twee factor authenticatie) en verscherpte werkprocessen te zorgen. Vraag uw medewerkers een nieuw sterk wachtwoord voor de Wifi-verbinding aan te maken. Ook niet onbelangrijk: zorg ervoor dat uw software up to date blijft en getest wordt.

Tip #3 Maak een risico-inschatting voor kritieke functies

De piek van het aantal zieken is op dit moment nog niet bereikt. Grote kans dat ook uw medewerkers ziek zullen worden en langere tijd afwezig zullen zijn. Wij adviseren u daarom om een overzicht te maken van kritieke functies en na te denken over mogelijke oplossingen voor het geval dat deze medewerkers ziek worden. Ook adviseren wij u om een prioriteitenlijst aan te maken voor de primaire processen en te zorgen dat er voor deze werkzaamheden redundantie in personeel is.

Tip #4 Pas de beveiliging van uw bedrijf aan

Als gevolg van het huidige thuiswerkbeleid staan veel kantoorgebouwen (grotendeels) leeg. Ook de bezetting van de beveiliging en receptie van veel bedrijven is op dit moment minder. Dit brengt risico's op diefstal en fraude met zich mee. Daarom adviseren we u om diefstalgevoelige middelen in kaart te brengen en deze te beveiligen, bijvoorbeeld in een afgesloten kast of kamer. Ook is het goed om de beveiliging en receptie te vragen extra controlerondes te lopen en afdelingen waar geen medewerkers werken af te sluiten en op het alarm te zetten. Maken uw medewerkers gebruik van andere in- en uitgangen om afstand van elkaar te kunnen houden? Zorg dan dat ook deze toegangsdeuren extra gecontroleerd worden.

Tip #5 Blijf vooruit denken

In een crisis als de huidige is het goed om vooruit te blijven denken. Wat gebeurt er als de huidige situatie langer aanhoudt dan verwacht? Of als de maatregelen komende weken onverhoopt nog scherper worden? Wat betekent dat voor uw bedrijf? En hoe kunt u zich daar nu al op voorbereiden?

Meer tips?

Wilt u meer tips? In het corona tweeluik op onze website vindt u meer informatie. Mocht u specifiekere ondersteuning wensen, neem dan contact met ons op. Wij helpen u graag!

Lokmiddelen oplossing tegen diefstal

Het inzetten van GPS bakens om voertuigen te volgen met behulp van satellieten is voor velen niet meer vreemd.

Track & Trace kent echter veel meer toepassingen die door Hoffmann ingezet kan worden. Zo is het ook mogelijk om producten te volgen, voor klanten die te maken hebben met structurele diefstallen.

Een voorbeeld: een bedrijf schakelde ons in omdat hij last had van regelmatig terugkerende diefstallen van consumentenelektronica. Wij prepareerden een bluetooth speaker als lokmiddel. De betrokkene nam de speaker op zijn werk weg en via de zendmasten kon de route gevolgd worden. In de buurt van de eindbestemming werd de Wifi actief en kon vastgesteld worden dat de weggenomen speaker zich in een flatgebouw bevond. Met behulp van een RFID functie (radiofrequentie) kon feilloos de voordeur aangewezen worden van de woning waarin de speaker zich bevond.

Een lokmiddel is altijd maatwerk, ze zijn in allerlei formaten en vormen te verkrijgen. De mallen worden digitaal getekend waarna zij digitaal geprint worden. Kleur en uiterlijk worden afgestemd op het doel waarvoor zij zijn bestemd, waarna het ontwikkelde lokmiddel ingezet wordt.

Een ander recent voorbeeld: een klant is al jarenlang slachtoffer van metaaldiefstallen. In een restpartij koper werd een geprepareerde buis geplaatst als lokmiddel (zie foto). Op het moment dat de partij in beweging kwam 'ontwaakte' het lokmiddel. Het observatie team van Hoffmann ontving een e-mailbericht en een SMS en zij konden in een digitale omgeving direct de lading volgen.

Het onderzoek leverde drie betrokkenen op die zich al langere tijd bezig hielden met de koperdiefstallen. Een aanzienlijke partij die verzameld was, afkomstig van onze klant werd teruggevonden. Met de inzet van het observatieteam en de tactische onderzoekers leverden het onderzoek betrokkenen op die hun aandeel bekenden. Onze klant kon aansluitend passende, arbeidsrechtelijke maatregelen nemen.



De manier van toepassingen waarvoor lokmiddelen ingezet kunnen worden zijn oneindig, denk aan post- en pakketbezorging, voedsel- en warenindustrie, gebruik in warehouses, in kantooromgevingen (denk bijvoorbeeld aan loklaptops of loktelefoons), in vervoermiddelen (navigatiesystemen, maar ook in elektrische fietsen of scooters) en bouwmachines en gereedschap. Zelfs plaatsing in zeecontainers is mogelijk, zodat deze overal ter wereld gevolgd kunnen worden. We vertellen u er graag meer over.

In 5 stappen naar een effectief screeningsbeleid

Als organisatie bent u zich bewust van de risico's die uw organisatie kunnen raken en die direct invloed kunnen hebben op de resultaten van de organisatie. Hiervoor zijn wellicht al specifieke beheersmaatregelen getroffen en volgt de organisatie mogelijk een structureel risicomanagement proces. Een belangrijk onderdeel van dit proces is het screenen van personeel, omdat u daarmee heel gericht de interne risico's kunt beheersen. Het opstellen van een screeningsbeleid kan u daarbij helpen. Hoffmann schreef het whitepaper 'in 5 stappen naar een effectief screeningsbeleid' om als handleiding te gebruiken.

U kunt het document downloaden op onze website.



Een welverdiende pauze?

Een gemeente krijgt een melding van haar buurgemeente: een werkvoertuig van de gemeente staat steeds aan het eind van de middag op haar grondgebied. Ook nuttigen de medewerkers alcohol in het voertuig en rijden daarna weg. Een serieuze melding! Want alcoholgebruik onder werktijd is een reden voor ontslag. De gemeente schakelt ons in om onderzoek te doen.

Op zoek naar het werkvoertuig

Onze observanten gaan op pad en zien na een aantal pogingen het betreffende werkvoertuig inderdaad stilstaan buiten de eigen gemeente. Een incident of gebeurt dit vaker? In overleg met de opdrachtgever en de jurist zetten we een gps-baken in. Zo kunnen we het werkvoertuig monitoren zonder dat continue observatie noodzakelijk is. De gps-informatie toont een duidelijk patroon: het werkvoertuig rijdt ongeveer één uur en een kwartier voor het einde van de werktijd de gemeente uit. Vervolgens staat het voertuig één uur stil op steeds een andere plek in de buurgemeente. Een kwartier voor het einde van de werktijd rijdt het voertuig terug naar de eigen gemeente.

Twee overtredingen

Er is sprake van twee overtredingen waar een waarschuwing op staat. Ten eerste hebben de medewerkers met het gemeentelijke werkvoertuig de gemeente verlaten, terwijl dit niet mag. Daarnaast maken ze zich schuldig aan urenfraude. De uren die ze stilstaan in de andere gemeente schrijven ze namelijk gewoon op projecten weg.

Maar alcoholgebruik?

Onze opdrachtgever wil vooral vaststellen of de medewerkers ook daadwerkelijk alcohol drinken in het werkvoertuig. Daarom zijn onze observanten

ongeveer een half uur van tevoren aanwezig op de verwachte locatie. Daar bekijken ze alle prullenbakken en maken foto's van de inhoud. Als het werkvoertuig wegrijdt, gooien de medewerkers namelijk steeds iets in de prullenbak. De observanten treffen daarin inderdaad lege bierflesjes aan. Toch is het bewijs nog aan de dunne kant. Eén van onze medewerkers stapt de volgende dag op het werkvoertuig af om de weg te vragen. Onze medewerker draagt daarbij verborgen camera's. Camera's die op dat moment vastleggen dat de ambtenaren inderdaad alcohol drinken. Daarmee is het bewijs rond.

Overtuigend bewijs

De volgende dag confronteren we de twee ambtenaren met de bevindingen. Ze lijken zich niet bewust van de voorbeeldfunctie die ze hebben. En urenfraude? Nee, dat is niet zo. Ze werken zó hard op de dag om hun werk af te maken dat ze recht hebben op een extra pauze. Toch denkt de gemeente daar anders over. De twee ambtenaren worden ontslagen.



In dit whitepaper bieden we:

- meer informatie over het waarom en het nut van een screeningsbeleid;
- de 5 stappen om tot een gedegen screeningsbeleid te komen;
- de do's en dont's bij het opstellen;
- een klantcase van 'De Hypothekers Associatie'.

Het nut van een screeningsbeleid

Met behulp van screening kunnen de risico's die aan een specifieke functie verbonden zijn, worden bepaald. Het is belangrijk dat de veiligheids- en de organisatie worden geïntegreerd en naast u bovendien een betrokken houding richting uw medewerkers. Wij zijn steeds volier de bereikbaarste partij. Het is belangrijk dat organisaties om in een screeningsbeleid te voorzien te helpen en er wordt gevraagd en waargemaakt. Voor inrichting van screening is dit artikel een goede start. In de handleiding komt u alles over het nut van een screeningsbeleid.

Risico in beeld

Bij het opstellen van een screeningsbeleid wordt in kaart gebracht welke veiligheidsrisico's aan een functie zijn verbonden. Het is belangrijk dat de veiligheids- en de organisatie worden geïntegreerd en naast u bovendien een betrokken houding richting uw medewerkers. Wij zijn steeds volier de bereikbaarste partij. Het is belangrijk dat organisaties om in een screeningsbeleid te voorzien te helpen en er wordt gevraagd en waargemaakt. Voor inrichting van screening is dit artikel een goede start. In de handleiding komt u alles over het nut van een screeningsbeleid.

Proces vastleggen

Met een goed doordacht screeningsbeleid zorgt u ervoor dat u altijd op de hoogte en een goede manier om te communiceren met uw medewerkers. Het is belangrijk dat de veiligheids- en de organisatie worden geïntegreerd en naast u bovendien een betrokken houding richting uw medewerkers. Wij zijn steeds volier de bereikbaarste partij. Het is belangrijk dat organisaties om in een screeningsbeleid te voorzien te helpen en er wordt gevraagd en waargemaakt. Voor inrichting van screening is dit artikel een goede start. In de handleiding komt u alles over het nut van een screeningsbeleid.

Draagvlak creëren

Elk goed screeningsbeleid wordt met betrekking tot een organisatie voor screening te implementeren. Het is belangrijk dat de veiligheids- en de organisatie worden geïntegreerd en naast u bovendien een betrokken houding richting uw medewerkers. Wij zijn steeds volier de bereikbaarste partij. Het is belangrijk dat organisaties om in een screeningsbeleid te voorzien te helpen en er wordt gevraagd en waargemaakt. Voor inrichting van screening is dit artikel een goede start. In de handleiding komt u alles over het nut van een screeningsbeleid.

Transparantie

Een screeningsbeleid moet ook voor medewerkers die niet betrokken zijn en medewerkers die niet betrokken zijn. Het is belangrijk dat de veiligheids- en de organisatie worden geïntegreerd en naast u bovendien een betrokken houding richting uw medewerkers. Wij zijn steeds volier de bereikbaarste partij. Het is belangrijk dat organisaties om in een screeningsbeleid te voorzien te helpen en er wordt gevraagd en waargemaakt. Voor inrichting van screening is dit artikel een goede start. In de handleiding komt u alles over het nut van een screeningsbeleid.

Bijdrage van onze partner Capra advocaten, door mr. Paula Berends

Kleine misdragingen en de zware normschending

Veel medewerkers zijn sterk betrokken bij het onderwijs waar zij werkzaam zijn. Dat geldt voor het primair onderwijs net zo goed als voor het MBO of voor de Universiteit. Die sterke betrokkenheid levert loyale en gedreven professionals op met hart voor de zaak. De betrokkenheid kan echter ook te ver gaan als een medewerker, in zijn streven om het goede te doen, toch een grens overschrijdt.

In de praktijk komen diverse misdragingen voor:

- Een docent (MBO) verlaat zijn groep ondanks de uitdrukkelijke instructie om bij zijn groep te blijven (maart 2019, aanslag Utrecht);
- Een docent (MBO) beweegt een ouder om niet de inkoopprijs te berekenen voor het leveren van barbecuebenodigdheden, maar de volle prijs. Het verschil zou ten goede komen aan een schoolproject waar de docent zich voor inzette. Dit is ook gebeurd. De speciale regels voor dit soort bijdragen van ouders is de docent niet nagekomen. Hij heeft geen enkel overleg met de school gevoerd en heeft alles op eigen houtje geregeld;
- Een docent (PO) schrijft herhaaldelijk via whatsapp "ik mis je" aan een leerling (8e groep) die naar het voortgezet onderwijs gaat;
- Een docent (SO) voert nevenwerkzaamheden uit (buitenschoolse opvang/individuele begeleiding van leerlingen) en zet deze voort ondanks het gebod van de werkgever om deze activiteiten te staken;
- Een facilitair medewerker (WO) gebruikt een dienstauto voor privé doeleinden.

Bij deze misdragingen ligt een zware maatregel (ontslag) niet in alle gevallen voor de hand. Hoe de misdragingen worden beoordeeld hangt af van de vraag of er naast die ene normoverschrijding nog sprake is van andere factoren. Zo kan een eerder gegeven waarschuwing ertoe leiden dat een relatief klein vergrijp toch zwaarder wordt bestraft. Verschillende misdragingen bij elkaar kunnen als een zware normschending worden aangemerkt, waar dan een zwaardere maatregel tegenover staat. De werkgever in kwestie moet in de eerste plaats een deugdelijk onderzoek (laten) uitvoeren naar de feiten, deze vervolgens goed analyseren en voorzien van een kwalificatie, voordat tot een arbeidsrechtelijke maatregel kan worden besloten.

In de zaak van de hiervoor genoemde facilitair medewerker (WO) was naast het privé gebruik van de dienstauto tevens sprake van leugenachtig gedrag en het wegnemen van goederen die de Universiteit toebehoorden. Camerabeelden, inloggegevens, de administratie van werkbonden en verschillende verantwoordingsgesprekken maakten onderdeel uit van het onderzoek. De normschendingen werden door de Universiteit in samenhang als zeer ernstig beoordeeld waarna strafontslag volgde.

Ontslag op staande voet was aan de orde in het geval van een directeur voor Primair Onderwijs die zijn werkgever jarenlang had voorgelogen over het bestaan van een stichting waaraan geld was overgemaakt dat de school toebehoorde. Ook had hij zijn eigen bankrekening 'gespekt'. In deze situatie is de financiële administratie uitvoerig onderzocht en zijn onderzoeksinterviews gehouden. De normschending was zeer ernstig en vormde een dringende reden voor ontslag.

In het geval van een conciërge die de inkomsten uit de externe verhuur van schoolruimtes voor zichzelf hield,

zich door de leerlingenvereniging had laten uitbetalen terwijl tevens overuren waren geschreven, en de melding van nevenactiviteiten achterwege had gelaten, lag het allemaal net wat anders. Fraude, zo oordeelde de werkgever en verzocht om ontbinding van de arbeidsovereenkomst wegens ernstig verwijtbaar handelen. De werkgever had gesprekken gevoerd, verklaringen op doen stellen en de computer van de conciërge doorzocht. Uit dit onderzoek leek te volgen dat de conciërge terecht verwijten waren gemaakt. Toch werd het verzoek tot ontbinding afgewezen. Betrokkene had namelijk gehandeld overeenkomstig mondelinge afspraken die eerder over externe verhuur waren gemaakt; hij bleek geen overuren te hebben geschreven; en de verplichte melding van nevenwerkzaamheden was onduidelijk geredigeerd. Voor wat betreft het onderzoek van de computer van betrokkene trof de werkgever zelf een verwijt. Het toepasselijke reglement had de werkgever namelijk naast zich neer gelegd. Het geschreven beleid van de werkgever kwam aldus niet overeen met hoe de regels in de praktijk werden toegepast.

Bij een vermoeden van een normschending is naast deugdelijk onderzoek voor een houdbaar ontslag dan ook tevens vereist dat de norm waaraan de werknemer zich moet houden, actueel is en actief wordt uitgedragen. Papier is geduldig, maar alleen met een praktische toepassing van het integriteitsbeleid kunnen kleine misdragingen en zware normschendingen adequaat worden aangepakt.

Capra Advocaten is actief betrokken bij de vormgeving, implementatie en handhaving van integriteitsbeleid, waaronder begrepen bijstand bij de arbeidsrechtelijke sanctionering van integriteitsschendingen.

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 gesprekken 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.