HOFFMANN TIPS

voor bedrijfsleven en publieke sector

Column
€ 19 miljoen weg door nepmails. En dan?

Casus:
Diefstal van poststukken en bestanden van de bedrijfscomputer/systemen

Casus:
Uitgebreid onderzoek naar informatiebeveiliging

Schepen onder vuur. De nieuwe dreiging!

CEO-fraude, een eenvoudige maar gevaarlijke vorm van fraude

Met gedrag en cultuur CEO-fraude voorkomen

Een gokverslaving zet aan tot factuurfraude

Risicomanagement, leren om andersom te redeneren

Ziekteverzuimcontrole, een dienst die actueel blijft

Kleine bedragen, grote gevolgen. Ontslag op staande voet?

#236
december 2018

COLUMN

€ 19 miljoen weg door nepmails. En dan?

Afgelopen maand kwam de CEO-fraude bij bioscoopketen Pathé uitgebreid in het nieuws. Criminelen wisten ruim € 19 miljoen buit te maken. Een succes voor de oplichters en een voorbeeld dat ongetwijfeld doet volgen. Want dit is een makkelijke manier van geld verdienen! Vanuit Hoffmann doen we gemiddeld 50 keer per jaar onderzoek naar dit soort situaties van CEO-fraude. Hoe heeft de fraude kunnen gebeuren? En waarom zijn de medewerkers in de betreffende casus afgeweken van het normale proces? Soms weten we door snel handelen de bankrekening van een oplichter te bevriezen en zo de schade te beperken.

Toch blijft er vaak een belangrijke vraag onbeantwoord: slachtoffer geworden van CEO-fraude en nu? Ik zie dat veel bedrijven na een CEO-fraude weer overgaan tot de orde van de dag. De onoplettende medewerker heeft een reprimande gekregen of is zelfs ontslagen. Dit zal ons niet meer gebeuren is de gedachte. Maar waarom niet? Zoals gezegd, CEO-fraude is voor oplichters een lucratieve business. Dit gaat in de toekomst nog veel vaker voorkomen. Belangrijk dat u op dit soort situaties bent voorbereid. Hoe? We delen een aantal ideeën met u in het artikel over de preventieve aanpak na CEO-fraude op pagina 5.

Natuurlijk delen we zoals gewoonlijk ook weer een aantal casussen en andere actuele onderwerpen met u. Zoals over informatiebeveiliging, ziekteverzuim en een schip dat gehackt wordt. Ik wens u veel leesplezier!

Martijn van de Beek

CASUS

Diefstal van poststukken en bestanden van de bedrijfscomputer en systemen

Bij een bedrijf komt men erachter dat al enige tijd post niet ontvangen wordt die wel verstuurd zou moeten zijn. Doordat de post niet aankomt lopen een aantal cruciale processen gevaar. Er wordt besloten om op een strategische plek een discreet aangebrachte camera aan te brengen om vast te stellen wie hiervoor verantwoordelijk is. Al snel was op de beelden te zien dat een medewerker van de afdeling Boekhouding de post op zijn bureau sorteerde en vervolgens enkele stukken in zijn koffer deed en die mee naar huis nam.

Wat men daarnaast op de beelden zag was dat de man uit zijn bureaulade een usb stick nam, deze in zijn computer stak en vervolgens handelingen op het toetsenbord uitvoerde. De gedachte was al snel dat de man bestanden aan het downloaden was. Het downloaden had geen enkele functionele reden en was zelfs verboden door de directie. De stick ging vervolgens in de koffer mee naar huis. De opdrachtgever schrok nog meer bij het bekijken van de beelden toen men zag dat de man ook achter de computer van één van directieleden ging zitten en ook daar met een usb stick in de weer ging. Het leek er sterk op dat er ook van die computer zaken naar de usb stick werden gekopieerd.
Tijd voor een digitaal onderzoek. Onze digitale rechercheurs hebben een uitgebreid onderzoek ingesteld. Uiteindelijk bleek dat de man zeer vertrouwelijke bestanden aan het kopiëren was geweest.

Met behulp van een gespecialiseerde advocaat werd er een digitaal bewijsbeslag aangevraagd bij de rechtbank om met behulp van een deurwaarder in de woning van de boekhouder een onderzoek uit te voeren. Zowel op de computer van de man, als in administratie om te kijken of er poststukken werden aangetroffen. Dit verlof werd door de rechtbank gegeven. Op de dag en het tijdstip dat de deurwaarder zich toegang mocht

verschaffen in de woning van de boekhouder zijn twee van onze rechercheurs met de boekhouder aan tafel gegaan om te kijken wat de reden van zijn handelen is geweest. De man bleek een tijd geleden de indruk te hebben gekregen dat men hem wilde gaan ontslaan. Om zijn vertrek financieel gezien zo goed als mogelijk te laten verlopen en uit boosheid omdat men een tweede boekhouder wilde aannemen was hij overgegaan tot deze handelingen.

Ontslag op staande voet was het gevolg. De computer thuis bij de man werd vakkundig ontdaan van alle onterechte bestanden en de poststukken die er nog lagen werden ingenomen.

Uitgebreid onderzoek naar informatiebeveiliging

Hoffmann werkt regelmatig voor rekenkamers binnen Nederland. De rekenkamers onderzoeken de doeltreffendheid, de doelmatigheid en de rechtmatigheid van het gevoerde bestuur van gemeenten en provincies. Het afgelopen jaar hebben we meerdere keren onderzoek gedaan naar de informatiebeveiliging van gemeenten en provinciën.

Onderzoeken als deze hebben vaak eenzelfde opzet. Het start meestal met een pentest op het interne netwerk. Hoe ver komt de ethical hacker zonder enige vorm van toegang (blackbox) te hebben?
In het tweede deel van deze pentest wordt er gebruik gemaakt van een testaccount die door de gemeente of provincie ter beschikking wordt gesteld (greybox). Onze medewerker krijgt een gebruikersaccount met weinig rechten om vervolgens het systeem te testen hoe ver hij binnen kan dringen. Is het bijvoorbeeld mogelijk om vanuit deze account admin-rechten te krijgen of mailboxen over te nemen.

Vervolgens gaat het onderzoek verder met een pentest op het wifi netwerk. Veel organisaties zijn zich niet bewust van de beveiligingsrisico's die draadloze netwerken met zich meebrengen. Soms is het mogelijk om via een gastennetwerk op het normale netwerk te komen.

Een zeer belangrijk onderdeel van onze informatie-beveiligingstesten is Social Engineering. Door middel van deze test wordt het veiligheidsbewustzijn van de medewerkers getest. Er wordt gestart met een phishing e-mailing om te proberen om inloggegevens van een brede groep medewerkers te achterhalen. Naast een brede phishing actie zetten we ook een spear phishing aanval op die gericht is op een beperkt aantal medewerkers. In een e-mail wordt een geïnfecteerde bijlage meegestuurd. Door de bijlage te openen krijgen wij toegang tot de systemen.

Naast deze digitale technieken maken we ook gebruik van fysieke tests bijvoorbeeld een inlooptest. Een mystery guest zal proberen om een gebouw binnen te komen en de beveiliging te omzeilen. Als je als hacker bijvoorbeeld de systemen niet van buiten af kan bereiken door goede beveiligingsmaatregelen dan lukt het wellicht wel van binnenuit. Ook kan het mogelijk zijn om informatie of informatiedragers zoals laptops mee te nemen als je eenmaal binnen bent. Deze uitkomsten zijn vaak verrassend, met een 'goed' verhaal en een vriendelijk gezicht kan je ver komen blijkt uit de ervaring.

De resultaten van onze onderzoeken worden geclassificeerd in kritiek-, hoog-, midden- en laag risico. Hoffmann adviseert vervolgens welke maatregelen direct en welke maatregelen er structureel genomen moeten worden.

> Daar 100% veiligheid niet bestaat, is het doel van informatieveiligheid de risico's tot een vastgesteld acceptabel niveau terug te brengen. De maatregelen die daarvoor genomen worden, moeten in verhouding staan tot de grootte van het risico.
> *Provincie Limburg*

Wat kan er gebeuren als je een schip gaat hacken?

Een internationaal bedrijf benaderde ons met de vraag om een grote olietanker te hacken. Voor de vestiging in Nederland hebben we al diverse pentesten en phisingmails uitgevoerd, altijd tot tevredenheid. Met deze niet alledaagse vraag gingen we graag aan de slag.

Het kantoor in Nederland heeft een directe netwerk-verbinding met het schip waar ter wereld deze ook vaart. De vraag was of iemand via dat netwerk het schip kan hacken. En vooral belangrijk als dat antwoord 'ja' zou zijn, wat valt er dan te bewerkstelligen op het schip. Verschillende scenario's kwamen ter sprake:

- Wat als milieuactivisten de regie over het schip kunnen voeren, dan wordt het bedrijf enorm chantabel.
- Stel, de besturing van het schip kan overgenomen worden en dit valt in handen van terroristen. Dan kan er een grote ramp plaatsvinden door het schip te laten verongelukken.
- Als de software bevroren kan worden, kunnen hackers veel geld eisen om dit weer vrij te geven, de schade kan enorm oplopen.
- Als de hacker tot de vertrouwde bedrijfsinformatie kan komen kunnen waardevolle gegevens worden gelekt naar concurrenten die er veel zijn in deze markt.

De eerste aanval van ethical hackers vanuit Hoffmann vond begin dit jaar plaats in de situatie zoals het bedrijf er toen voor stond. De hackers slaagden erin om het netwerk van het schip binnen te komen. Zij konden systemen aan- en uitzetten, dus de geschetste scenario's kwamen dichtbij. Tijd voor actie, het bedrijf heeft een Intrusion Prevention System geïnstalleerd.

De tweede aanval vond rond de zomer plaats en het systeem deed zijn werking, de hackers konden niet meer in het systeem komen. Wel werden er nog enkele kwetsbaarheden geconstateerd in de configuratie. Een advies volgde hoe dit op te lossen waar het bedrijf mee aan de slag is gegaan.

Einde van het jaar volgt de derde aanval, als alle adviezen zijn opgevolgd, zou dat betekenen dat de aanval niet gaat slagen.

CEO-fraude, een eenvoudige maar gevaarlijke vorm van fraude

Begin september was het veelvuldig in het nieuws, CEO-fraude is een eenvoudige maar zeer effectieve vorm van fraude die steeds meer voorkomt. Een aantal bekende organisaties kwam ermee in het nieuws. Zo werden de algemeen en financieel directeur van bioscoopketen Pathé ontslagen nadat zij slachtoffer werden van CEO-fraude. Ondanks dat beide personen hun twijfel hadden over de gang van zaken maakten zij toch in totaal ruim € 19 miljoen over naar een fraudeursbende.

Dat deze fraudevorm sterk groeiende is lijkt duidelijk. Alleen al binnen Hoffmann is het aantal dossiers vervier-voudigd in vergelijk met 3 jaar geleden en de bedragen die buit worden gemaakt lopen enorm op, soms tot in de miljoenen zoals in het omschreven voorbeeld.

Werkwijze

Deze vorm van fraude wordt vaak onderschat vanwege zijn eenvoud. Mensen denken al snel dat ze daar niet in trappen. Maar de werkwijze van de fraudeurs is zo geprofessionaliseerd dat de kans steeds groter wordt. In veel gevallen wordt bij CEO-fraude de e-mailbox van de CEO gehackt door middel van een phishingmail. De fraudeur kan inloggen in de e-mailbox en verstuurt vervolgens een e-mail naar een financiële medewerker met het verzoek om een spoedbetaling te verzorgen. Vervolgens voert de fraudeur de druk snel op. In korte tijd stuurt hij meerdere e-mails met vragen over de status van de betaling. In de meeste gevallen is er een relatief grote hiërarchische afstand tussen de CEO en de medewerker van de financiële afdeling. Daardoor is de kans klein dat de medewerker contact opneemt met de CEO om de juistheid van de betalingsopdracht te controleren. In zijn e-mails legt de fraudeur bovendien de nadruk op het geheime karakter van de betaling. Daardoor is de kans groot dat de financieel medewerker de betaling daadwerkelijk uitvoert.

Op het gebied van techniek adviseren wij u om te werken met multiple authentication, ofwel inloggen via twee soorten devices.

Als het hacken van de e-mailbox niet lukt dan wordt er vanuit een valse domeinnaam gemaild welke verdacht veel lijkt op het echte e-mailadres.

Voorbeeld valse domeinnaam

Een financieel medewerker kreeg een mail van de CEO vanuit China met het verzoek om een betaling van $ 255.000 te doen. De fraudeur heeft in dit geval gebruik gemaakt van een domeinnaam die erg lijkt op de originele domeinnaam. In plaats van .cn stond er .ch. Het kleine verschil werd niet opgemerkt door de betreffende medewerker en na een korte mail-wisseling is het geld netjes overgemaakt naar het genoemde bankrekeningnummer. Nadat deze betaling was ontvangen hebben de fraudeurs geprobeerd met een phishing mail een andere mailbox te hacken om meer nog buit te maken. Dat werd gelukkig wel opgemerkt waardoor ze geen tweede bedrag hebben overgemaakt.

Preventieve maatregelen

Ondanks de slinkse manier van werken zijn er een aantal preventieve maatregelen te nemen om je te wapenen tegen de fraudeurs, zowel op de organisatorische-, technische- als op de menskant. Het is belangrijk om allereerst de procedures te bekijken hoe er om wordt gegaan met betalingen binnen het bedrijf. En nog belangrijker: worden deze procedures ook nageleefd. Veel organisaties werken met een vier-ogen principe waarbij er altijd twee medewerkers een betaling checken voor hij wordt gedaan. Maar vaak zorgt snelheid ervoor dat deze procedure niet wordt gevolgd of wordt omzeild. Maak uw medewerker niet alleen bewust van de gevaren maar zorg dat ze hun gedrag aanpassen om zo veilig mogelijk te werken.

Op het gebied van techniek adviseren wij u om te werken met multiple authentication, ofwel inloggen via twee soorten devices. Na het invoeren van het wachtwoord krijg je een pushbericht op je mobiele telefoon die geaccordeerd moet worden om daadwerkelijk in het systeem te komen. Dit zorgt ervoor dat de kans op hacken wordt geminimaliseerd.

Daarnaast zal op het moment dat de medewerkers zich bewust zijn van de gevaren een valse domeinnaam sneller worden opgemerkt.

Met gedrag en cultuur CEO-fraude voorkomen

Na een incident als CEO-fraude gaan veel bedrijven weer over tot de orde van de dag. En dat is begrijpelijk, want zo'n vervelend incident leidt alleen maar af van de core business. Toch blijft de vraag: bent u als organisatie veiliger geworden na één incident van CEO-fraude? Weten wat er gebeurd is, is niet genoeg. Wij dagen onze klanten uit om in zo'n situatie een laag dieper te kijken. Naast de technische maatregelen is het van groot belang om de mens te bekijken want deze is vaak de zwakste schakel. Wat bevordert of belemmert de medewerkers in het volgen van processen? Zo'n follow-up maakt uw organisatie pas echt veiliger. Ook bij een poging tot CEO-fraude in de toekomst.

Analyse van de situatie

Vaak hebben medewerkers bij CEO-fraude wel hun twijfels, maar ze doen niets met die twijfels. Waarom zijn medewerkers niet kritisch? Heerst er een cultuur van opdrachten uitvoeren of staat men juist open voor een kritische houding van de medewerker op de werkvloer? De processen zijn vaak helder omschreven, maar de cultuur en het gedrag van mensen heeft invloed op het resultaat. De vraag is: hoe kunt u uw medewerkers weerbaarder maken?

Afspraken maken voor gewenst gedrag?

Onze sociaal psychologen doen met het Hoffmann gedragsprogramma een uitgebreid onderzoek binnen uw organisatie. Door middel van interviews spreken zij verschillende medewerkers. Zo krijgen zij boven tafel wat de knelpunten zijn, waarom er wordt afgeweken van procedures. De uitkomsten van de gesprekken worden omgezet in concrete adviezen over maatregelen die te treffen zijn. En dat gaat niet altijd om dure of tijdrovende maatregelen. Maak bijvoorbeeld de afspraak om bij twijfel

altijd te bellen met de afzender. Plak het op de muur! Uiteraard moet de baas dan wel aanspreekbaar zijn. In een helder 3x3 model worden de adviezen gepresenteerd zodat u uw organisatie weerbaar maakt.

Een gokverslaving zet aan tot factuurfraude

Een bank vindt het opvallend dat één van zijn klanten tot vijf keer aan toe veel geld op zijn rekening krijgt bijgeschreven. Gezien deze persoon altijd in de schulden heeft gestaan wordt dit niet vertrouwd. Niet alleen zwom hij ineens in het geld, maar hij loste zijn hypotheek af en al zijn overige schulden die hij bij de bank had openstaan.

De bank benadert hierop de partij waar het geld van afkomstig is. Wat blijkt is dat dit de werkgever is van de klant die al zijn schulden heeft afgelost. De werkgever wist niets van de betalingen, waarna er een fraude-onderzoek wordt gestart.

Er vindt een uitgebreid digitaal onderzoek plaats en op basis van de resultaten gaan twee van onze rechercheurs met de medewerker in gesprek. Het blijkt al snel dat het onderzoek de juiste bevindingen heeft opgeleverd, want de medewerker bekent direct dat hij verantwoordelijk is voor de betalingen van zijn werkgever naar zijn eigen rekening.

De medewerker werkt al twintig jaar op de Crediteuren-administratie van het bedrijf. Bij zijn werkgever wordt bekend dat hij te maken heeft met een gokverslaving. Om die reden werden zijn rechten beperkt en kon hij zelfstandig geen betalingen meer verrichten. Maar via een achterdeur kon hij wel stamgegevens aanpassen in het systeem. Dat gaf de opening voor de fraude. Meneer stond op het punt om zijn woning uitgezet te worden en wist zich geen raad meer. De hoogste betaling die klaarstond heeft hij vervalst en via een omweg uit het zicht gezet. Dat lukte de eerste keer direct en met de € 300.000 die hij had overgeboekt, kon hij zijn schulden aflossen. Hij wist dat aan het einde van het jaar de betaling van deze € 300.000 aan het licht zou komen bij het opmaken van de jaarbalans. Mede daarom heeft hij nog vier keer het bedrag overgemaakt en geprobeerd het geld te verdubbelen via goksites. Hiermee hoopte de medewerker aan het einde van het jaar het geld terug te betalen, eventueel met rente. Maar het geluk stond niet aan zijn zijde, er is geen cent meer over van de anderhalf miljoen euro die hij buit heeft gemaakt. Alles is vergokt.

Risicomanagement: leren om andersom te redeneren

‘Voorkomen is beter dan genezen’, misschien wel dé lijfspreuk voor een preventieve houding in iedere branche. Het voorkomen van incidenten is wenselijk voor elke organisatie. Incidenten hebben invloed op de personen die er mee te maken hebben, op het imago van de organisatie en het kan zelfs financiële gevolgen voor uw organisatie hebben.

Bij Hoffmann zien we in de praktijk dat veel organisaties zich pas bewust worden van de risico’s die ze lopen, nadat er zich een incident heeft voorgedaan. Dit incident wordt vervolgens de start van een proces waarin maatregelen genomen worden die het incident in de toekomst moeten zien te voorkomen. Hoewel het goed is om te leren van fouten, wie is er niet groot geworden met trial and error, kan het soms beter zijn om fouten niet te maken. Of; om te weten hoe je als organisatie moet reageren op het moment dat er zich een fout – incident – voordoet.

Organisaties zijn echter snel geneigd om zich over te geven aan de ‘oplossings-impuls’: handelen op basis van een directe oplossing voor het specifieke probleem wat zich voordoet. Enkele voorbeelden zijn:

- Het plaatsen van één enkele camera op het raampje dat bij de vorige inbraak is gebruikt om binnen te komen;
- Het plaatsen van een compleet hekwerk rondom een school ter voorkoming van inbraak en diefstal van laptops, waar men mogelijk had volstaan met de aanschaf van een kluis waar de laptops in passen;
- Het inzetten van verscherpte toegangscontrole met inzet van extra beveiligers naar aanleiding van diefstal van de koperen leidingen op de daken van de fabriek, terwijl deze inmiddels vervangen zijn door een ander metaal en het risico op diefstal verder klein is.

Hoffmann ondersteunt bedrijven in het structureel aanlopen van een dergelijk risicoproces. Wij zijn in staat om niet alleen te reageren op hetgeen wat al mis is gegaan, maar wij werken graag met u aan het inzichtelijk krijgen waar uw organisaties risico’s loopt. Net zoals bedrijven een product op de markt brengen vanuit een marktanalyse, brengt Hoffmann u een maatwerktraject gebaseerd op een analyse van uw bedrijf. In dit traject op maat worden:

- de kroonjuwelen van uw organisatie (bedrijfsgevoelige informatie, een grondstof, een kritiek bedrijfsmiddel, technische informatie, een cruciale bedrijfsapplicatie of bijvoorbeeld geld) geanalyseerd,
- de risico’s die uw organisatie loopt in kaart gebracht,
- uw huidige kwetsbaarheid ten opzichte van die risico’s weergegeven,
- en ontvangt u concrete aanbevelingen die uw organisatie beter bestand maken tegen deze risico’s.

Samen met u, creëren we zo een gestructureerd plan van aanpak richting de toekomst. Een maatwerktraject dat uw specifieke risico’s in kaart brengt en effectieve beveiligingsmiddelen inzet. Want niet iedere organisatie heeft baat bij een torenhoog hek, een toegangscontrole systeem en camera’s. Dit proces geeft u de mogelijkheid om voor de feiten uit te lopen, en om concrete stappen te zetten om incidenten binnen uw organisatie te voorkomen.

Ziekteverzuimcontrole, een dienst die actueel blijft

Controle op ziekteverzuim is één van de diensten binnen Hoffmann die al jarenlang wordt uitgevoerd en nog altijd actueel is. Wanneer u sterke vermoedens heeft dat een medewerker zich onterecht ziek heeft gemeld dan kunt u een onderzoek laten uitvoeren.

- **Wit verzuim:** de werknemer is daadwerkelijk ziek of arbeidsongeschikt en kan daarom de werkzaamheden niet uitvoeren. Dit is aantoonbaar door middel van een bedrijfsarts, psycholoog, ziekenhuis etc.;
- **Zwart verzuim:** de werknemer meldt zich ziek en voert zijn werkzaamheden niet uit, maar hij is niet ziek en gewoon in staat het werk te verrichten;
- **Grijs verzuim:** De werknemer meldt zich ziek met reële klachten, maar het staat niet vast dat de werknemer niet tot werken in staat is. Het is dan ook moeilijk voor de organisatie om de werknemer arbeid te laten verrichten. De werknemer wel op werk laten verschijnen, waar hij vervolgens geen of nauwelijks werkzaamheden verricht, dus improductief is, wordt ook grijs verzuim genoemd.

Er is te allen tijde een gerechtvaardigd belang nodig om een controle op ziekteverzuim te starten, een onderbuikgevoel is niet voldoende. Het is van belang dat u een dossier aanmaakt met duidelijke signalen waaruit zou blijken dat er sprake is van onterecht ziekteverzuim. Soms is één signaal al wel voldoende zoals in dit geval:

Een medewerker ziet zijn 'zieke collega' een straatje leggen en rapporteert dat aan zijn werkgever. Deze collega kon zijn werk niet uitvoeren omdat hij enorm last van zijn rug had en zit daarom ziek thuis. Een duidelijk geval van zwart verzuim en in dit voorbeeld is er dan ook een gerechtvaardigd belang om een onderzoek te starten.

In sommige gevallen voeren wij eerst een informatief onderzoek uit, gevolgd door een observatie. Observatie is één van de zwaarste middelen om in te zetten tijdens een onderzoek. Bij observatie worden er persoonsgegevens verwerkt, wat betekent dat de persoon die wordt geobserveerd altijd in kennis gesteld moet worden dat er onderzoek naar hem of haar is gedaan. Het is wettelijk verplicht. Om het onderzoek goed uit te kunnen voeren kan de in kennisstelling uiteraard achteraf plaatsvinden.

Een werkgever ziet in een winkel één van zijn medewerkers die al langdurig ziek is vanwege een slechte knie. De winkel waarin hij zich begeeft is van de vrouw van de werknemer en nadat hij is aangesproken door zijn werkgever geeft hij aan dat hij slechts op bezoek is. De werkgever vertrouwt dit niet en schakelt Hoffmann in voor een onderzoek. De observatie wordt gepland waarbij er op 5 verschillende dagen een bezoek aan de winkel wordt gebracht. Op 4 van de 5 dagen is de betrokkene in de winkel en voert hij werkzaamheden uit zoals het vullen van schappen of het afrekenen bij de kassa.

Onze rechercheurs bekijken dus of de zieke werknemer activiteiten uitvoert die niet conform de afspraken zijn. Soms is een 'zieke' medewerker tijdens zijn ziekteperiode aan het werk voor een andere werkgever, in dit geval zijn vrouw. Rechercheurs maken wanneer nodig onopvallend foto's en video's en noteren hun bevindingen. U ontvangt een rapport met de onderzoekresultaten én het beeldmateriaal. In het volgende voorbeeld gaat de betrokken medewerker nog een stap verder.

Bij een schoonmaakbedrijf is een medewerker al langdurig ziek. Deze persoon wordt gespot in een wit busje met een ladder op het dak en de opdrachtgever vermoedt dat hij voor iemand anders werkt. Er wordt een onderzoek ingesteld waarin de man wordt geobserveerd. Hij rijdt met zijn busje naar verschillende opdrachtgevers van zijn werkgever. Wat blijkt, hij is een eigen bedrijfje gestart en heeft zichzelf voor een lager tarief aangeboden. Deze man is ontslagen en heeft alle gemaakte kosten van zijn werkgever moeten betalen.

BIJDRAGE VAN ONZE PARTNER LEXENCE, DOOR FRANK TER HUURNE

Kleine bedragen, grote gevolgen. Ontslag op staande voet?

In een recente zaak heeft het Hof 's Hertogenbosch zich uitgelaten over de volgende vraag: is het ontslag op staande voet van een monteur die voor eigen rekening oud ijzer verkoopt voor een bedrag van € 38,- rechtsgeldig? De casus: de werkgever is een bedrijf dat supermarkten, winkels en bibliotheken inricht. Indien restmaterialen retour komen, wordt beoordeeld of deze voor hergebruik geschikt zijn, dan wel of de restmaterialen afgevoerd dienen te worden. De werkgever behaalt inkomsten met het inzamelen en (laten) afvoeren van de af te voeren restmaterialen, waaronder oud ijzer.

Nadat een vrachtwagen van de werkgever kort vermist was, is het tracking en tracing systeem van de vrachtwagen geraadpleegd. Daaruit bleek dat de vrachtwagen op een adres was geweest waar een metaalhandel is gevestigd. De werkgever heeft daarop een onderzoeksbureau de opdracht gegeven een onderzoek in te stellen naar het afvoeren en verkopen van oud ijzer.

Uit het onderzoek is gebleken dat de voertuigen van de werkgever zich in een periode van twee jaar meer dan 100 keer hebben begeven naar metaalhandelaren waarmee de werkgever geen overeenkomst had en zonder dat daartoe door de werkgever opdracht was gegeven. Vervolgens heeft een gesprek plaatsgevonden tussen het onderzoeksbureau, de werkgever en de betrokken werknemer (een monteur). De monteur heeft tijdens het gesprek toegegeven wel eens oud ijzer te hebben verkocht. De werkgever heeft de werknemer daarop op staande voet ontslagen.

In eerste aanleg heeft de kantonrechter geoordeeld dat het ontslag op staande voet rechtsgeldig is en een schadevergoeding en een vergoeding voor de onderzoekskosten toegewezen. De monteur is vervolgens in hoger beroep gegaan.

De monteur voert in hoger beroep onder meer aan dat verkochte restmaterialen niet als bedrijfsmiddelen kunnen worden aangemerkt. Het hof gaat daar niet in mee en oordeelt dat de monteur waarde heeft onttrokken aan de onderneming. Daarbij maakt het niet uit of het gaat om 'restmaterialen' of 'bedrijfsmiddelen'. Het hof overweegt dan ook dat de dringende reden is komen vast te staan.

Het gaat in deze zaak over handelen van de monteur dat heeft geleid tot een financiële benadeling van de werkgever, waarvan de monteur zich bewust was of had moeten zijn. Het vertrouwen van de werkgever in de monteur is daardoor ernstig beschadigd, terwijl de werkgever moet kunnen vertrouwen op de integriteit van de werknemers. De monteur was bovendien al eerder door de werkgever aangesproken op het meenemen van lampen. Hier komt bij dat, naar het oordeel van het hof, het bij de verkoop van oud ijzer voor een totaalbedrag van € 53 tot € 68 niet gaat om een verwaarloosbaar bedrag. Bovendien: uit rechtspraak volgt dat wanneer sprake is van diefstal van een goed van beperkte (financiële) waarde – de zogenaamde "bagateldelicten" – een strenge benadering wordt gevolgd. Diefstal is diefstal. Het is dan wel van belang dat de werkgever een strikt beleid toepast en de werknemers bekend zijn met dit beleid en de consequenties van overtreding.

Het hof oordeelt tot slot dat de kantonrechter de gevorderde onderzoekskosten ten onrechte heeft toegewezen. Volgens het hof zijn deze kosten aan te merken als kosten ter vaststelling van schade en aansprakelijkheid in de zin van artikel 6:96 lid 2 sub b BW. Dergelijke kosten worden alleen voor vergoed indien zij 'redelijk' zijn.

De werkgever had echter de onderzoekskosten onvoldoende onderbouwd. Een belangrijke tip voor werkgevers: bij procedures waarin onderzoekskosten zijn gemaakt kunt u (of uw advocaat) de rechter verzoeken om een vergoeding van deze onderzoekskosten.
Let erop dat dit verzoek goed gemotiveerd moet zijn!

Intermezzo: voor een rechtsgeldig ontslag op staande voet moet aan drie vereisten zijn voldaan: (1) er moet een dringende reden voor ontslag zijn, (2) het ontslag moet onverwijld (direct) worden gegeven nadat de werkgever de dringende reden heeft ontdekt en (3) de dringende reden moet onverwijld worden medegedeeld aan de werknemer.

Lexence advocaten & notarissen

Hoffmann-Tips voor bedrijfsleven en publieke sector is een periodieke uitgave van

Hoffmann

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