HOFFMANN TIPS

voor bedrijfsleven en publieke sector

#245 | Juni 2022

Goed werkgeverschap in deze tijd

- *Casus: Alwéér voorin?*
- *Klant Open Line vertelt over de uitgevoerde pentest*
- *Interactieve Workshop Sociale Veiligheid*
- *Privacy: waarom u toch iets te verbergen heeft.*

Hoffmann

Column

Goed werkgeverschap in deze tijd

Vorig jaar kon ik nog tanken voor minder dan 2 euro per liter. Tegenwoordig betaal ik heel wat meer. De prijzen in de supermarkt stijgen. De prijzen voor energie en gas stijgen. Om de huidige inflatie kunnen we niet heen. We hebben te maken met een inflatie die we in geen jaren hebben gezien. Een inflatie die bij lange na niet gecompenseerd wordt in stijging van de lonen. Wat mij zorgen baart, is dat hierdoor een deel van de bevolking financieel klem komt te zitten.

Voedingsbodem voor fraude en ongewenst gedrag
Medewerkers die het financieel zwaar hebben, komen makkelijker in de verleiding om te frauderen. Fraude en ongewenst gedrag worden namelijk beïnvloed door gelegenheid, motivatie en capaciteit. De motivatie neemt nu bij een deel van de bevolking toe, omdat die financieel klem komt te zitten. Volgens mij ligt hier een kans voor werkgevers om invulling te geven aan goed werkgeverschap. Wat kunnen we als werkgever doen in deze tijd?

Gelegenheid verminderen en zorgen voor medewerkers
We kunnen de verleiding wegnemen door te zorgen voor minder gelegenheden om te frauderen. Dit betekent kritisch naar de eigen processen en procedures kijken. Moet u uw medewerkers bijvoorbeeld met contant geld laten werken? En zo ja, hoe maakt u de gelegenheid op verleiding dan zo klein mogelijk?

Daarnaast geloof ik dat we verleiding kunnen voorkomen door signalen serieus te nemen. In hoeverre weten we als werkgever wat er bij onze medewerkers speelt? Is hulp aanbieden iets wat in uw organisatie aan de orde komt? Gaan we in gesprek bij een loonbeslag of bij andere signalen die wijzen op schulden? Door met elkaar in gesprek te zijn, is het mogelijk om op zoek te gaan naar de win-win. Hierdoor daalt de motivatie om te frauderen. Misschien kan de medewerker bijvoorbeeld tijdelijk wel extra uren maken.

Alternatieven bieden
Kleine vormen van ongewenst gedrag kunnen grote gevolgen hebben. Welke vormen van ongewenst gedrag doen zich voor in uw organisatie die u vrij eenvoudig kunt oplossen? Ik moet in dit kader denken aan een casus bij een klant die ambulancezorg verleende. Tegen de zomerperiode verdwenen daar vaak de verloopstekkers waarmee apparatuur wordt opgeladen. Slechts een klein ding van nog geen vijftien euro. Wat is het probleem dan? Het gevolg was echter dat apparatuur niet meer kan worden opgeladen waardoor de zorg tekortschoot. In dit geval loonde het voor deze werkgever om mee te denken met de medewerkers. Zij kunnen nu voor hun caravan of aanhanger een verloopstekker lenen als ze op vakantie gaan.

Tot slot
Ongewenst gedrag doet zich voor in alle soorten en maten. Juist in deze tijd waarin het voor sommige medewerkers lastiger is om de verleiding te weerstaan, kunnen we als werkgever helpen.

Veel leesplezier!

Martijn van de Beek

Alwéér voorin?!

Natuurlijk is er bij een brandweereenheid in het noorden van het land af en toe sprake van een geintje onderling. Maar nu is er ook echt sprake van pestgedrag. Het onklaar maken van een brandweerpak, schoenen verstoppen, water in de schoenen. Het zijn voorbeelden van pesterijen die ervoor zorgen dat opgepiepte brandweermannen niet mee kunnen op de brandweerwagen. Daarnaast valt het diverse brandweermannen op dat één collega wel heel vaak voorin zit als bevelvoerder bij een uitruk. Dat is verdacht, want het computersysteem zorgt er juist voor dat de verdeling van taken random maar ook evenredig gebeurt. Er klopt duidelijk iets niet. De leidinggevende besluit om ons in te schakelen voor een onderzoek.

Gesprekken op de werkvloer

We beginnen ons onderzoek door gesprekken te voeren met een flink aantal directe collega's. Wat is er precies aan de hand? Niemand die dat weet. Wel krijgen we allerlei concrete voorvallen boven tafel. Bovendien valt het op dat de naam van één collega wel heel vaak genoemd wordt. Het is een beginnend bevelvoerder die met horten en stoten door de opleiding is gekomen. Hij zit vol ambitie. Het is opvallend dat iedereen dezelfde persoon verdenkt, maar wij werken liever met concreet bewijs.

Het computersysteem onder de loep

Bij de volgende stap in ons onderzoek doen we een grondige analyse in het computersysteem. Dit systeem piept de brandweermensen op bij een noodgeval. Iedereen die reageert dat hij naar de kazerne komt, krijgt op de kazerne te horen of hij wel of niet meegaat in de wagen. Het computersysteem bepaalt dit. Ook bepaalt het wie welke taak heeft: chauffeur, bevelvoerder of manschap. Het computersysteem is zo ingericht dat iedereen evenredig aan de beurt komt. Wat blijkt als wij het computersysteem goed bekijken? De administrator heeft een flink aantal wijzigingen aangebracht in het computersysteem. Wijzigingen die in het voordeel van de administrator werken. En u voelt het misschien al aankomen: de administrator is de ambitieuze, beginnend bevelvoerder.

Gesprek met de betrokkene

Onze bevindingen leggen we zo snel mogelijk voor aan de betreffende brandweerman. Hij bekent geknoeid te hebben in het systeem, zodat hij zelf vaker als bevelvoerder mee kon bij een alarmmelding. Daarmee heeft hij zichzelf bevoordeeld. Maar de andere pesterijen ontkent de betrokkene. Voor de leidinggevende is de optelsom van alle opgehaalde informatie, in combinatie met het feit dat er geen draagvlak meer is voor deze persoon, genoeg reden om de man op non-actief te stellen. Ook heeft de brandweer aangegeven afscheid te willen nemen van deze brandweerman.

Medewerkers met schulden, hoe voorkomt u dat zij frauderen?

De redenen om fraude te plegen zijn per persoon anders, maar het valt ons bij Hoffmann de laatste tijd op dat veel betrokkenen een forse schuldenpositie hebben, zonder dat de werkgever daarmee bekend is. Medewerkers met forse schulden zijn vaak gevoeliger voor omkoping, diefstal en fraude. Hoe kunt u nu voorkomen dat uw bedrijf hiermee te maken krijgt?

Cijfers schuldenproblematiek
Om u inzicht te geven hoe groot de schuldenproblematiek in Nederland eigenlijk is, hebben we een aantal cijfers voor u op een rij gezet:

- Ruim 5 miljoen mensen hebben geen spaargeld. Dit betekent dat zij geen tegenslagen kunnen opvangen en niet kunnen investeren.
- Ruim 30% van de huishoudens heeft een betalingsachterstand.
- Ruim 614.000 huishoudens staan geregistreerd met problematische schulden. Dit zijn meer dan 1 miljoen mensen die hun schulden niet meer op eigen kracht kunnen wegwerken.
- Van deze groep krijgt slechts 14% hulp, bijvoorbeeld via de schuldhulpverlening. De rest probeert zelf uit de schulden te komen.
- Gemiddeld duurt het 5 jaar voordat iemand met financiële problemen hulp inroept.

Dit zijn forse aantallen. Maar het werkelijke aantal huishoudens met problematische schulden ligt naar alle waarschijnlijkheid nog hoger. Sommige mensen blijven namelijk onder de radar, bijvoorbeeld omdat zij geld hebben geleend bij familieleden of kennissen en daardoor niet geregistreerd staan.

Overigens is er op dit moment geen sterke toename van de schuldenproblematiek te zien door corona. Dit zegt echter niet zoveel; bij de financiële crisis van 2008 kwamen veel problemen pas jaren later aan het licht. Bovendien zijn veel ondernemingen tot nu toe overeind gehouden door de steunmaatregelen van de overheid. Nu deze maatregelen zijn geëindigd en vanaf oktober 2022 ook de belastingschulden weer moeten worden terugbetaald, verwachten schuldhulpverleners dat het aantal huishoudens met problematische schulden de komende tijd fors zal toenemen.

Voorbeelden uit de praktijk

- *Een medewerker met een schuld van € 70.000 komt er zelf niet meer uit. Ze besluit zich ziek te melden en als ZZP'er aan de slag te gaan. Daardoor verzekert zij zich van een dubbel inkomen en hoopt zo haar schulden sneller af te kunnen lossen.*

- *Een medewerker van de afdeling inkoop heeft een schuld van ruim € 50.000. Om deze schuld af te kunnen betalen, besluit hij extra goederen in te kopen en deze thuis af te laten leveren. De facturen accordeert hij zelf en komen voor rekening van de werkgever. De goederen verkoopt hij, om met de opbrengst zijn schuld af te kunnen lossen.*

- *Een medewerker met forse gokschulden heeft een tegenvaller gehad. Voordat hij bij zijn werkgever in dienst kwam had hij een eigen bedrijf, dat nu slapende is. Hij besluit het bedrijf weer nieuw leven in te blazen en gaat met de bedrijfsmiddelen van zijn werkgever aan de slag voor zijn opdrachtgevers.*

Hoe kunt u diefstal, omkoping en fraude voorkomen?
Er zijn verschillende manieren waarop u diefstal, omkoping en fraude door medewerkers met schulden kunt voorkomen:

1. Een belangrijk middel om de schuldenpositie van potentiële werknemers aan het licht te brengen is de pre-employment screening van kandidaten. De afgelopen jaren hebben we gezien dat vanwege de coronapandemie veel medewerkers zijn aangenomen na een verkorte procedure en een enkel sollicitatiegesprek via Teams of Zoom. Een pre-employment screening werd daarbij veelal achterwege gelaten. Het is belangrijk om deze screenings nu op te pakken, ook in de huidige krappe arbeidsmarkt.

2. Tijdens de coronapandemie hebben we ook gezien dat medewerkers vanwege het werken op afstand meer vrijheden en bevoegdheden hebben gekregen. Ook de medewerkers die zijn aangenomen zonder pre-employment screening. Het blijft dus belangrijk om toegekende rechten en bevoegdheden periodiek na te lopen en het betalingsverkeer steekproefsgewijs te controleren en in te passen in de AO/IC.

3. Als u erachter komt dat een kandidaat of medewerker (problematische) schulden heeft, hoeft dit niet automatisch te betekenen dat u deze kandidaat niet kunt aannemen of het contract niet moet verlengen. De arbeidsmarkt is tenslotte al krap genoeg. In plaats daarvan kunt u ook met de medewerker in gesprek gaan en uw hulp aanbieden. Deze aanpak kent ook andere voordelen: grotere betrokkenheid van uw medewerker bij uw bedrijf, minder ziekteverzuim en minder productieverlies als gevolg van stress en (daardoor) minder functioneren.

Maar welke hulp kunt u dan concreet bieden? Om te beginnen is het belangrijk om een veilige omgeving te creëren waarin medewerkers over hun financiële problemen kunnen praten zonder dat ze bang hoeven zijn voor ontslag of het niet verlengen van hun arbeidsovereenkomst. Bent u eenmaal in gesprek met een kandidaat of medewerker met schulden? Dan kunt u hem of haar doorverwijzen naar het Nibud, waar verschillende opleidingen en vormen van ondersteuning verkrijgbaar zijn. Ook kunt u de medewerker doorverwijzen naar de schuldhulpverlening van de gemeente of als werkgever zelf een Nibud-coach inschakelen.

Casus

Een mol op de werkvloer

Binnen een maand tijd vertrekken er drie medewerkers van een technisch productiebedrijf. De opzeggingen komen als een verrassing. Ineens vloeien commerciële kennis, product- en marktkennis en leidinggevende capaciteiten weg uit het productiebedrijf. En dat niet alleen. Niet veel later blijkt dat ook de offerteaanvragen stagneren. Er worden minder offertes aangevraagd en minder orders gegund. Per toeval komt de directeur van het productiebedrijf erachter dat één van de medewerkers van de binnendienst een offerteaanvraag doorstuurt naar zijn privémail. Zonder dat hij hiervan iets op de klantkaart schrijft. Onze opdrachtgever ruikt onraad.

Digitaal onderzoek
Na een uitgebreid intakegesprek beginnen wij met ons onderzoek. Uit het digitale onderzoek blijkt dat de desbetreffende medewerker van de binnendienst wel vaker offerteaanvragen naar zijn privémail stuurt. Stelselmatig zelfs. En geen van die offerteaanvragen vermeldt hij op de klantkaarten. Daarnaast ontdekken we dat er kort voor het vertrek van de drie andere medewerkers een grote datadump is gemaakt door één van hen. We kunnen achterhalen dat deze data zijn opgeslagen op een usb-stick die niet van het bedrijf zelf was. De datadump betreft klantgegevens, inkoopprijzen, marges en vertrouwelijke tekeningen. Absoluut de 'kroonjuwelen' van dit bedrijf, gegevens die essentieel zijn voor het bedrijfsproces.

Verder onderzoek en observaties
Uit ons informatieve onderzoek blijkt dat er een concurrerend bedrijf is opgericht. Als we de bedrijfsgegevens goed bekijken, stellen we vast dat de drie ex-medewerkers én de huidige medewerker van de binnendienst aandeelhouder zijn in dat concurrerende bedrijf. We besluiten observaties uit te voeren. Want: waar produceert men? En wie is er nog meer betrokken? Tijdens de observaties zien we ook twee andere medewerkers binnenlopen die nog in dienst zijn van het productiebedrijf.

Confronterende gesprekken
Op basis van ons vooronderzoek voeren we confronterende gesprekken met de medewerkers die op dat moment nog in dienst zijn bij het productiebedrijf. Al snel komt de aap uit de mouw: het was de bedoeling van de ex-medewerkers om een concurrerend bedrijf op te zetten en een mol in de organisatie achter te laten. Doordat ze extra handen nodig hadden voor een aantal opdrachten, hadden ze de twee medewerkers benaderd.

Een harde les
Onze opdrachtgever neemt afscheid van de medewerker van de binnendienst en de twee andere medewerkers die nog in dienst zijn. Het vertrouwen is weggeslagen. De rechter kent verlof toe voor een digitaal bewijsbeslag. Uiteindelijk blijkt dat de vertrokken leidinggevende in het verleden al een soortgelijke actie heeft uitgevoerd. Pijnlijk is dat dit met een pre-employmentonderzoek naar boven zou zijn gekomen. Een harde les die ervoor zorgt dat onze opdrachtgever daar nu meer aandacht aan besteedt.

Open Line

Hackers zoeken dagelijks naar nieuwe manieren om organisaties binnen te dringen. Zij worden hierin steeds creatiever én succesvoller. Met een pentest kunt u laten onderzoeken of uw organisatie voldoende weerbaar is tegen deze aanvallen en krijgt u inzicht in de kwetsbaarheden van uw IT-infrastructuur.

Een van de bedrijven die een pentest door Hoffmann heeft laten uitvoeren is managed service provider Open Line. In deze casus vertellen Eric IJpelaar, Security & Privacy Officer bij Open Line, en Mathijs, ICT Security Consultant bij Hoffmann, over die samenwerking.

Pentesting
Eric: "Ik vergelijk een pentest vaak met een inbraak in een woning. Voordat een inbreker overgaat tot de inbraak, gaat hij altijd eerst op zoek naar kwetsbaarheden aan de woning. Een kiepraampje, een slot dat makkelijk te forceren is of een raam met enkel glas. Een pentest is in die zin niet anders. Een pentester gaat in feite ook op zoek naar een achterdeurtje of openstaand raam om de systemen binnen te komen."

"Dat is inderdaad wel een goede vergelijking", aldus Mathijs. "Bij een pentest probeer ik via technische en organisatorische kwetsbaarheden in te breken in de computersystemen van de klant. Denk daarbij aan verouderde besturingssystemen of een gebrekkige beveiligingsupdate, maar ook aan de combinatie van een e-mailadres en een wachtwoord. Dat kan een wachtwoord zijn dat betrokken is geweest bij een datalek of een zwak wachtwoord als 'Welkom123' of 'Welkom2022!'. Eenmaal binnen probeer ik vervolgens, afhankelijk van de opdracht, zo ver mogelijk in de systemen binnen te dringen. Bij IT-beheerders zoals Open Line probeer ik ook in de stepping stone omgeving van hun klanten te komen. Na afloop maak ik een rapportage op met bevindingen en aanbevelingen. Maar als ik tijdens de opdracht op een groot risico stuit, meld ik dat natuurlijk direct."

Eric: "Wij zijn managed service provider van een honderdtal bedrijven en organisaties, van lokale overheden en zorginstellingen tot woningbouw-corporaties en ondernemingen in de productie, logistiek en handel". Goede informatiebeveiliging is een belangrijk onderdeel van ons visitekaartje. Daarom laten wij regelmatig pentests uitvoeren. Met de aanbevelingen die daar uit volgen kunnen we onze beveiliging én die van onze klanten continu blijven verbeteren."

Samenwerking Hoffmann & Open Line
Mathijs: "Eric en ik zijn met elkaar in contact gekomen via een klant van Open Line, waar ik een pentest uitvoerde."
Eric: "Wij moesten daarbij ondersteunen en vanuit die contacten zijn wij zelf ook met Hoffmann in zee gegaan. Mathijs heeft nu twee keer een pentest bij Open Line uitgevoerd. Op dit moment zijn we intern in gesprek over wat we komend jaar gaan doen. Mogelijk komt er ook nog een stukje social engineering bij."

"In de IT-industrie is het best practice om ieder jaar een andere pentester te nemen, maar daar ben ik geen voorstander van," vervolgt Eric. "Een pentester heeft maar beperkt de tijd, in die korte periode kan hij niet van alle ins en outs van een bedrijf op de hoogte zijn. Als je een pentester vaker inzet, kent hij de omgeving al en is de

kans groter dat hij nieuwe zwakheden boven tafel brengt. Ik ben van mening dat als het écht je doelstelling is om je beveiliging te verbeteren, je wel op deze manier moet werken. Veel bedrijven laten echter een pentest uitvoeren om een 'compliance vinkje' te kunnen zetten. Die zitten er eigenlijk niet echt op te wachten om geconfronteerd te worden met eventuele zwakheden."

Op de vraag wat Eric's ervaringen met Hoffmann zijn antwoordt hij: "De samenwerking met Mathijs verloopt goed. Tijdens de pentest hebben we regelmatig contact. En als hij zijn conceptrapportage af heeft, lopen we altijd samen door de bevindingen heen en kijken we welke mitigerende maatregelen er mogelijk zijn. Het is een illusie om te denken dat een pentester niets vindt, Mathijs vindt altijd iets. Maar dat doet een hacker ook." "100% beveiliging bestaat niet", besluit Mathijs. "Je bent nu eenmaal afhankelijk van de factoren mens, techniek en organisatie. Zelfs als je het technisch en organisatorisch 100% op orde zou hebben, kunnen hackers via je medewerkers vaak alsnog binnenkomen."

"Een pentester gaat in feite ook op zoek naar een achterdeurtje of openstaand raam om de systemen binnen te komen."

Eric IJpelaar

Partner bijdrage

Heimelijk opnemen van gesprekken leidt tot einde dienstverband

Dit artikel is geschreven door Maartje Rutten, advocaat-partner bij Capra Advocaten. Uit recente rechtspraak blijkt (opnieuw) dat het door een werknemer stiekem opnemen van gesprekken met zijn werkgever kan leiden tot een verstoorde arbeidsrelatie en een ontbinding van de arbeidsovereenkomst. Wat waren de feiten?

De feiten

De werkneemster is in 2019 in dienst getreden als teamleider. In 2021 vond een functioneringsgesprek plaats tussen de werkneemster en haar leidinggevende. Van dit gesprek werd een verslag opgesteld. In het verslag was opgenomen dat de werkneemster was aangeboden om een opleiding te volgen. De werkneemster wijst dat aanbod af waarop de leidinggevende aangeeft dat het er bewust voor kiezen om zich niet verder te ontwikkelen, consequenties kan hebben voor het uitvoeren van de functie. Korte tijd later meldt de werkneemster zich ziek. Ondanks het advies van de bedrijfsarts geeft de werkneemster aan niet in gesprek te willen gaan met haar leidinggevende omdat dit voor haar ziekmakend is. Ook het aanbod tot mediation wijst de werkneemster af.

Opnemen gesprekken door werkneemster

Er volgen drie gesprekken tussen de werkneemster en haar leidinggevende. Hierbij is een derde aanwezig. Tijdens het laatste gesprek geeft de werkneemster aan dat zij de gevoerde gesprekken heeft opgenomen. Dat is voor de werkgever de welbekende druppel. Een voortzetting van het dienstverband is wat betreft de werkgever niet meer mogelijk. De kantonrechter wordt gevraagd om de arbeidsovereenkomst te ontbinden wegens een verstoorde arbeidsrelatie.

De rechter

Naar het oordeel van de rechter is de arbeidsverhouding tussen partijen duurzaam verstoord. Deze verstoring vindt volgens de rechter zijn oorsprong in het functioneringsgesprek. Aan de hand van opgestelde verklaringen van partijen constateert de rechter dat door deze verstoring een onwerkbare situatie is ontstaan.

Anders dan de werkneemster naar voren heeft gebracht, staat de omstandigheid dat er geen mediation is gepoogd, niet in de weg aan deze conclusie. De rechter oordeelt dat voldoende is gebleken dat de werkgever pogingen heeft gedaan om de verhouding te normaliseren door het voeren van gesprekken met de werkneemster. Mogelijk dat mediation in dat stadium nog aan bod had kunnen komen, maar de werkneemster heeft dat toen afgehouden. Het is de werkneemster geweest die door het heimelijk opnemen van gesprekken om de werkgever daar vervolgens mee te confronteren, de arbeidsverhouding definitief en onherstelbaar heeft verstoord.

Heimelijk opnemen gesprekken mag niet

Uiteindelijk doet het maken van heimelijke opnames de werkneemster de das om. Het stiekem opnemen van gesprekken met de werkgever kan dus leiden tot de conclusie dat sprake is van een verstoorde arbeidsrelatie met als gevolg het einde van de arbeidsovereenkomst. Over het stiekem opnemen van gesprekken door de werknemers, is vaker geprocedeerd. In meerdere zaken kwam de rechter tot het oordeel dat het heimelijk opnemen van gesprekken 'hoogst onfatsoenlijk is' en 'getuigt van een diepgeworteld wantrouwen'. In die zaken werd de arbeidsovereenkomst ontbonden wegens een verstoorde arbeidsrelatie.

Mogen gesprekken nooit worden opgenomen?

De uitspraken doen geloven dat gesprekken nooit mogen worden opgenomen. Dat is niet zo. Het is in beginsel immers niet onrechtmatig om gesprekken waaraan een werknemer zelf deelneemt, op te nemen. Maar zonder dit melden of te vragen voor het opnemen van gesprekken, is niet netjes en doet meestal ernstige afbreuk aan het vertrouwen. Dit kan eenvoudig worden voorkomen door voorafgaand aan een gesprek kenbaar te maken dat een opname wordt gemaakt.

capra advocaten overheid onderwijs zorg

Update vanuit cybersecurity-land

Datalekken

Mo Ballari
m.ballari@hoffmann.nl
06-47384377

Onze consultant cybersecurity Mo Ballari praat u iedere Hoffmann Tips bij over trends die op dit moment actueel zijn. Waar hij normaal gesproken meerdere trends bespreekt, staat deze editie geheel in het teken van datalekken.

Ze zijn de laatste tijd bijna dagelijks in het nieuws: datalekken. Persoonsgegevens die op straat belanden en daardoor in handen van onbevoegden. Steeds vaker is een datalek het gevolg van een cyberaanval. Het aantal bij de Autoriteit Persoonsgegevens gemelde datalekken als gevolg van een cyberaanval nam in 2021 met 88% toe, tot 2210. Wat je noemt een explosieve stijging!

Is het dan zo makkelijk om een succesvolle cyberaanval uit te voeren, of nemen organisaties onvoldoende maatregelen om een datalek te voorkomen? Waarschijnlijk is beide een beetje waar. Cybercriminelen worden zeker steeds bedrevener, maar tegelijkertijd hebben nog te weinig organisaties hun basisbeveiliging op orde.

Laat ik vooropstellen dat er geen wondermiddel bestaat om te voorkomen dat u getroffen wordt door een ransomware-aanval. Maar u kunt het cybercriminelen wel lastiger maken. Bijvoorbeeld met een goed beveiligingsplan, dat gebaseerd is op een risicoanalyse. In dit beveiligingsplan definieert u een set maatregelen uitgesplitst naar de factoren mens, techniek en organisatie. Maar let op: om een bepaald niveau van cyberveiligheid te bereiken, moet u een gelaagde verdediging opbouwen. Daarom is het van belang aandacht te besteden aan alle drie de factoren, niet alleen aan de techniek. Ik licht dit hieronder toe.

Techniek

Velen van u hebben het mij eerder horen zeggen: 'Cybersecurity bestaat bij de gratie van een goede beveiliging van de ICT systemen'. Dit begint allemaal bij een veilige configuratie, goed patchen en tijdig updaten. Maar ook multifactor authenticatie, encryptie en een goed autorisatiemodel in combinatie met monitoring-software zijn van groot belang. Net als de mogelijkheid om digitaal forensisch onderzoek te kunnen doen als er iets misgaat. Nog te veel organisaties bewaren hun loggegevens kort, vaak uit kostenoverwegingen. Maar daardoor zijn zij niet forensic ready en is er te weinig of helemaal geen onderzoeksmateriaal beschikbaar op het moment dat zich een datalek voordoet.

Organisatie

Daarnaast is een aantal organisatorische aspecten van belang voor een goede informatiebeveiliging. Weet u bijvoorbeeld aan welke wet- en regelgeving uw organisatie moet voldoen? Heeft u een informatiebeveiligheidsbeleid? Is er een plan voor het geval de organisatie te maken krijgt met een security-incident? Heeft u in- en uitdiensttredingsprocedures, waarin is beschreven welke rechten medewerkers krijgen en wanneer zij deze weer inleveren? Worden verleende rechten regelmatig gecontroleerd en herbeoordeeld? Laat u nieuwe medewerkers screenen, zeker als zij toegang krijgen tot vertrouwelijke of concurrentiegevoelige informatie?

Mens

Tot slot speelt de mens een cruciale rol in uw informatiebeveiliging. Het gedrag van uw medewerkers bepaalt namelijk in hoge mate of uw organisatie het slachtoffer kan worden van cybercriminelen. U kunt nog zo'n goede firewall hebben, op het moment dat medewerkers op een geïnfecteerd linkje klikken is de organisatie nog steeds kwetsbaar.

Het is dus van belang dat uw medewerkers zich bewust zijn van de risico's. Een cybersecurity-expert kan ze daar meer over vertellen. Maar als organisatie moet u uw medewerkers ook in staat stellen om cyberveilig gedrag te vertonen. Hier zijn verschillende methodes en technieken voor. Als u daar prijs op stelt, vertel ik u daar graag meer over.

Mo Ballari

Interactieve workshop Sociale Veiligheid

Sociale veiligheid op het werk; wat is dat eigenlijk? Is dat een werkomgeving waar adequaat wordt gereageerd op ongewenst gedrag? Een werkomgeving die gericht is op het voorkomen van ongewenst gedrag? Of een combinatie van beide?

Sociale veiligheid gaat over het bevorderen van een gezonde organisatiecultuur en het voorkomen van ongewenst gedrag. Sociale veiligheid betekent niet dat er nooit meer iets voorvalt, het betekent wel dat er ook in die gevallen adequaat gereageerd wordt om de situatie op te lossen.

Maar waarom zou u zich actief inzetten voor sociale veiligheid binnen uw organisatie? We geven u de drie belangrijkste redenen:

1. Het welzijn van uw medewerkers. Een ongezonde organisatiecultuur kan negatieve effecten hebben op het welzijn van uw medewerkers. Depressie, angst, agressie, slapeloosheid, concentratiestoornissen, psychosomatische klachten, burn-out klachten en (chronische) stress liggen op de loer.
2. De productiviteit van de organisatie. Bovengenoemde negatieve effecten kunnen op hun beurt negatieve gevolgen hebben voor de productiviteit, het ziekteverzuim en het personeelsverloop binnen de organisatie.
3. Uw juridische verantwoordelijkheid voor het creëren van een veilige werkplek. Op grond van de Arbowet bent u als werkgever verplicht om beleid te voeren dat gericht is op het voorkomen dan wel beperken van psychosociale arbeidsbelasting.

Om de sociale veiligheid binnen uw organisatie te verbeteren, heeft Hoffmann een interactieve Workshop Sociale Veiligheid ontwikkeld, waarin de volgende onderwerpen aan bod komen:

- Een veilige organisatiecultuur
- Het voorkomen van ongewenst gedrag (preventie)
- Het reageren op ongewenst gedrag (repressie)

Workshop op maat

Met de Workshop Sociale Veiligheid biedt Hoffmann een op maat gemaakt programma om sociaal veilig gedrag bij uw medewerkers te stimuleren en de leidinggevenden in uw organisatie te ondersteunen bij het uitdragen van een veilige organisatiecultuur. Hierbij worden de ervaring en expertise van onze psychologen ingezet om een aanpak aan te reiken die aansluit bij uw doelstellingen en organisatie.

Tijdens de workshop nemen zij uw medewerkers (op een interactieve wijze) mee in het begrip sociale veiligheid, verschillende vormen van ongewenst gedrag en de normen en waarden binnen uw organisatie. Voor uw medewerkers is het belangrijk om te beseffen en te respecteren dat de grens van (on)gewenst gedrag bij iedereen anders kan zijn. In de workshop voor leidinggevenden kan de nadruk (tevens) worden gelegd op het belang van voorbeeldgedrag.

Daarnaast wordt tijdens de workshop door de deelnemers geoefend met gesprekstechnieken die, afhankelijk van de doelgroep, vanuit twee invalshoeken belicht kunnen worden. Voor de doelgroep medewerkers richten de gesprekstechnieken zich op het aangeven van de eigen grenzen en het bespreekbaar kunnen en durven maken van ongewenst gedrag (assertiviteit). Voor de doelgroep leidinggevenden richten de gesprekstechnieken zich op het leiden van (gevoelige) gesprekken.

Sociale veiligheid kan een gevoelig onderwerp zijn binnen uw organisatie. Onze psychologen beschikken over de juiste vaardigheden om tijdens de workshop een veilige omgeving te creëren. Zij kunnen vanuit hun expertise bovendien adequaat inspringen op vragen en behoeften die tijdens de sessies naar boven kunnen komen.

Vragen

Heeft u hier vragen over? Neem dan gerust contact met ons op. De psychologen van Hoffmann gaan graag met u in gesprek en kunnen de workshop toespitsen op uw organisatie.

Ongewenst gedrag en het grijze gebied

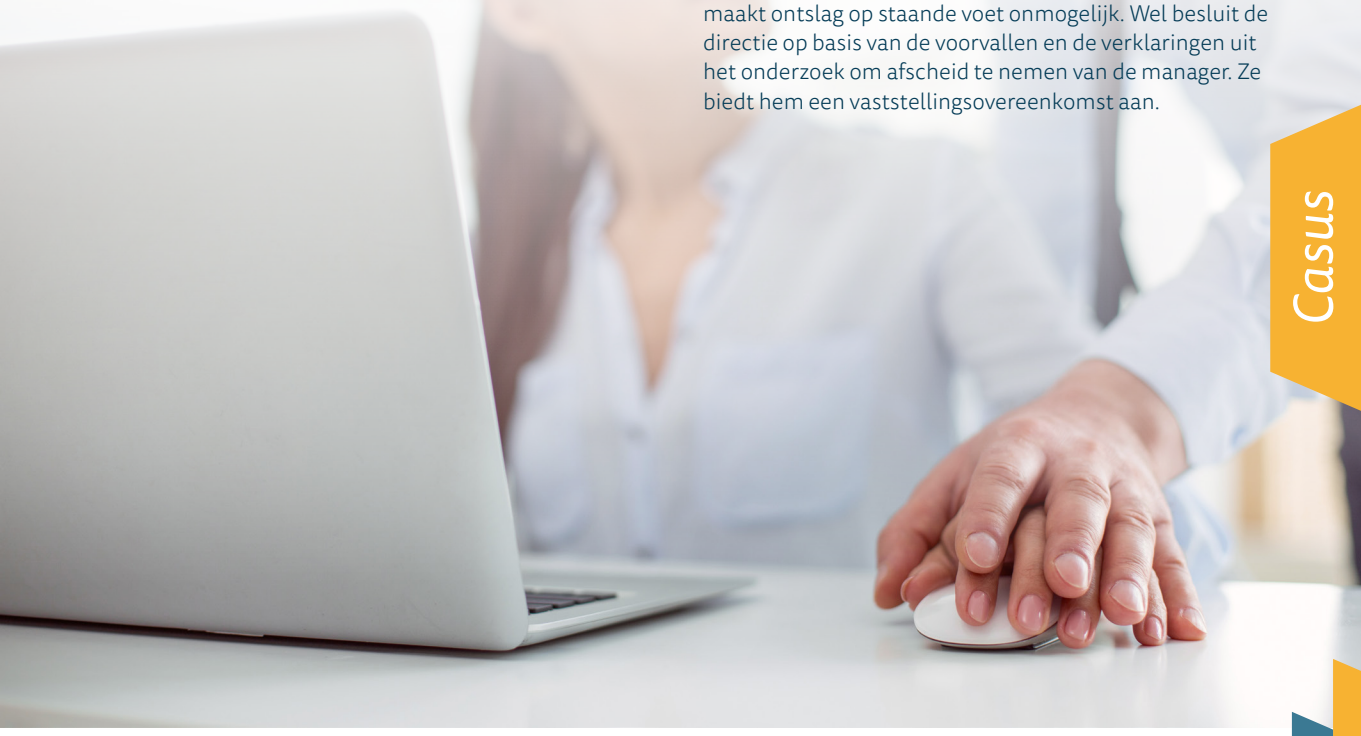
Bij een distributiecentrum in het westen van het land wordt extra kantoorpersoneel aangenomen. Er komen twee jongere dames in dienst als aanvulling op het team. Opvallend is dat deze twee dames kort na hun indiensttreding en onafhankelijk van elkaar een klacht indienen over het gedrag van hun manager. Het gaat over een manager die al een hele lange tijd bij het distributiecentrum werkt. Hoe kan het dat er opeens meldingen komen over deze manager? De directie neemt de meldingen serieus en schakelt ons in voor een zorgvuldig onderzoek.

Van de meldsters...
Na een voorbespreking met de opdrachtgever beginnen we ons onderzoek door beide dames, afzonderlijk van elkaar, te spreken. Elk van hen vertelt ons wat er precies is voorgevallen. Eén van hen vertelt dat ze nog steeds overstuur is door het voorval en er niet door kan slapen. Het is duidelijk dat de dames de voorvallen als grensoverschrijdend gedrag hebben ervaren. Er dient gedegen vervolgonderzoek plaats te vinden.

...naar de collega's.
Om een volledig beeld te krijgen van het gedrag van de manager spreken we ook met de andere medewerkers van de afdeling. Dat doen we door algemene vragen te stellen zonder een directe link naar de manager. Dit is nodig om het belang van de manager te beschermen. We vragen hen bijvoorbeeld of ze bekend zijn met ongewenst gedrag binnen het bedrijf. Zodra we naar voorbeelden vragen, komt de naam van de manager naar voren. De dames die er langer zitten, lijken overigens niet wakker te liggen van het gedrag van de manager. "Zo is hij nou eenmaal. Je moet gewoon een grapje terug maken."

Nog meer gesprekken...
Eén van de voorvallen had plaatsgevonden tijdens een vergadering. Daarom benaderen we ook de aanwezigen van die vergadering. Ook aan hen stellen we algemene vragen. Zij beamen dat het voorval had plaatsgevonden en dat het ongemakkelijk was. Ook spreken we met oud-leidinggevenden van de manager. Die geven aan dat de manager al diverse keren in het verleden is aangesproken op zijn gedrag. Helaas heeft daar nooit goede verslaglegging van plaatsgevonden.

...en een gesprek met de manager zelf.
Uiteindelijk spreken we natuurlijk ook met de manager zelf. Hij geeft aan dat het gewoon om een grapje ging. Dit laat het grijze gebied bij ongewenst gedrag zien: wanneer is iets een grapje en wanneer gaat het om grens-overschrijdend gedrag? Iedereen interpreteert dat anders. Zo gaan de wat oudere dames duidelijk anders om met het gedrag van de manager dan de jongere dames. Uiteindelijk geeft de manager zelf ook aan dat sommige van zijn 'grapjes' inderdaad te ver gingen. Helaas biedt de gedragscode van het distributiecentrum geen concrete handvatten voor de situaties die waren voorgevallen. Dat maakt ontslag op staande voet onmogelijk. Wel besluit de directie op basis van de voorvallen en de verklaringen uit het onderzoek om afscheid te nemen van de manager. Ze biedt hem een vaststellingsovereenkomst aan.



PRIVACY: WAAROM U TOCH IETS TE VERBERGEN HEEFT

'Ik heb toch niets te verbergen'; een vaak gehoord argument in discussies over privacy. De meeste mensen die dit argument gebruiken gaan ervan uit dat hun data te onbelangrijk is voor criminelen, overheden en bedrijven. Of dat deze partijen 'er toch niets mee kunnen'. Maar deze onverschilligheid komt voort uit onwetendheid. Want die mensen zien namelijk niet welke overheden, bedrijven en/of onbevoegden op onze (digitale) data jagen, hoe ze dat doen, waarom ze het doen, wat ze er uiteindelijk mee doen en hoe dit onze levens beïnvloedt. Kortom, we dénken niets te verbergen te hebben, maar als we toch eens wisten...

De Googles, Facebooks, Snapchats en Tiktoks van deze wereld kennen ons beter dan onze familie en vrienden. Al surfend op uw smartphone wordt u continue 'bespied' door honderden -vaak onbekende- bedrijven en/of organisaties. Zelfs als chatgesprekken, zoals WhatsApp, end-to-end gecodeerd worden.

Bij Hoffmann vinden we privacy te belangrijk om af te doen als iets wat alleen criminelen of onbevoegden nodig hebben. Om veiliger met uw eigen data en smartphone(s) om te gaan en de impact van mogelijk 'bespieden' te kunnen verkleinen, geven we u dan ook graag enkele beveiligingsaanbevelingen.

Algemene aanbevelingen

- Google uzelf eens in de zoveel tijd.
- Check uw e-mailadres geregeld op www.haveibeenpwned.com om te controleren of het is gelekt op internet.
- Gebruik sterke wachtwoorden en gebruik verschillende wachtwoorden voor verschillende websites of applicaties. U kunt ook een wachtzin gebruiken. Zinnen zijn makkelijk te onthouden en lang.
- Deel wachtwoorden niet met anderen, zoals vrienden of collega's. En gebruik een wachtwoordmanager.
- Gebruik indien mogelijk altijd twee factor authenticatie (2FA) bij het inloggen op gebruikte websites/diensten. 2FA is veelal in te stellen onder het account van de websites/diensten zelf, onder het kopje 'beveiliging'. Gebruik hierbij de applicaties 'Authy' of 'Authenticator' (van Google), die u op de smartphone kunt installeren. Maak geen gebruik van de optie om u een beveiligingscode via sms te laten toesturen, omdat deze code door onbevoegden kan worden afgevangen.
- Deel zo min mogelijk via e-mailberichten. E-mailberichten zijn niet gecodeerd en hebben geen end-to-end encryptie.
- Gebruik zo min mogelijk gratis e-maildiensten zoals Gmail of Hotmail. Bij gratis diensten bent u als gebruiker het product. Van Google is bekend dat ze 'meelezen' met de inhoud van e-mailberichten en ook metadata verzamelen van e-mailberichten.

Aanbevelingen gebruik smartphone

- Update uw smartphone altijd zo snel mogelijk.
- Herstart uw smartphone geregeld opnieuw.
- Verwijder niet gebruikte applicaties regelmatig.
- Controleer applicaties met online accounts geregeld. Zonder dat u het beseft, geeft u deze applicaties vaak volledig toegang tot uw account, maar een applicatie kan gehackt worden.
- Controleer welke rechten applicaties hebben, zoals toegang tot de microfoon of locatie. Dit kunt u checken via 'Instellingen'.
- Zet 'tracking' van applicaties uit.
- Zet bluetooth, wifi en NF uit als u het niet gebruikt. Onbevoegden kunnen scannen op wifi en bluetooth zonder dat u het weet. Ook winkels en gemeenten doen dat, bijvoorbeeld om verplaatsingen in beeld te brengen.
- Vermijd zoveel mogelijk openbare wifi netwerken. Indien u gebruik wilt maken van een openbaar wifi-netwerk, gebruik dan een VPN (Virtual Private Network) verbinding. De best geteste en privacybeschermende VPN applicatie is Mullvad.

Aanbevelingen gebruik Social media, chat applicaties en bellen

- Bij het gebruik van WhatsApp of Signal:
  - Zorg dat berichten na enkele dagen of weken automatisch worden verwijderd. Dit kunt u instellen in de applicatie zelf, onder 'Instellingen'.
  - Zet het maken van back-ups uit. Back-ups worden standaard ongecodeerd opgeslagen in de cloud. Wanneer u wel een back-up in de cloud wilt maken, zet dan onder dezelfde Instellingen 'End-to-end versleutelde reservekopie' aan, zodat uw back-up gecodeerd in de cloud worden opgeslagen.
  - Schakel onder 'Instellingen' -> 'Privacy' de verschillende opties voor 'Iedereen' uit en zet deze minimaal op 'Mijn contacten'. Hiermee voorkomt u dat iedereen u kan benaderen.
  - Schakel onder 'Privacy' ook 'Live locatie' uit.
- Gebruik zoveel mogelijk social media applicaties via de webbrowser versie. Dit klinkt gek, maar de webbrowser is de meest veilige applicatie om op de smartphone te gebruiken.
- Zet social media accounts op privé en log uzelf uit als u de applicatie niet gebruikt.

Specialist aan het woord: ***Joost***

Na 22 jaar in de ICT te hebben gewerkt, is Joost nu al ruim 5,5 jaar Senior Onderzoeker Forensische IT bij Hoffmann.

Joost: "Ik houd mij bij Hoffmann onder meer bezig met de digitale component van fraudeonderzoeken. Vaak doe ik dat in samenwerking met de tactische recherche. Zo onderzoeken we onder meer CEO- en factuurfraude, maar doen we bijvoorbeeld ook onderzoek naar het lekken van gevoelige informatie of het gebruik van frauduleuze social mediaprofielen. De laatste tijd ervaren wij een groei in onderzoeken naar ransomware aanvallen. Dat is echt een hot item. We zien dat steeds meer bedrijven en overheden worden aangevallen, vaak vanuit het buitenland."

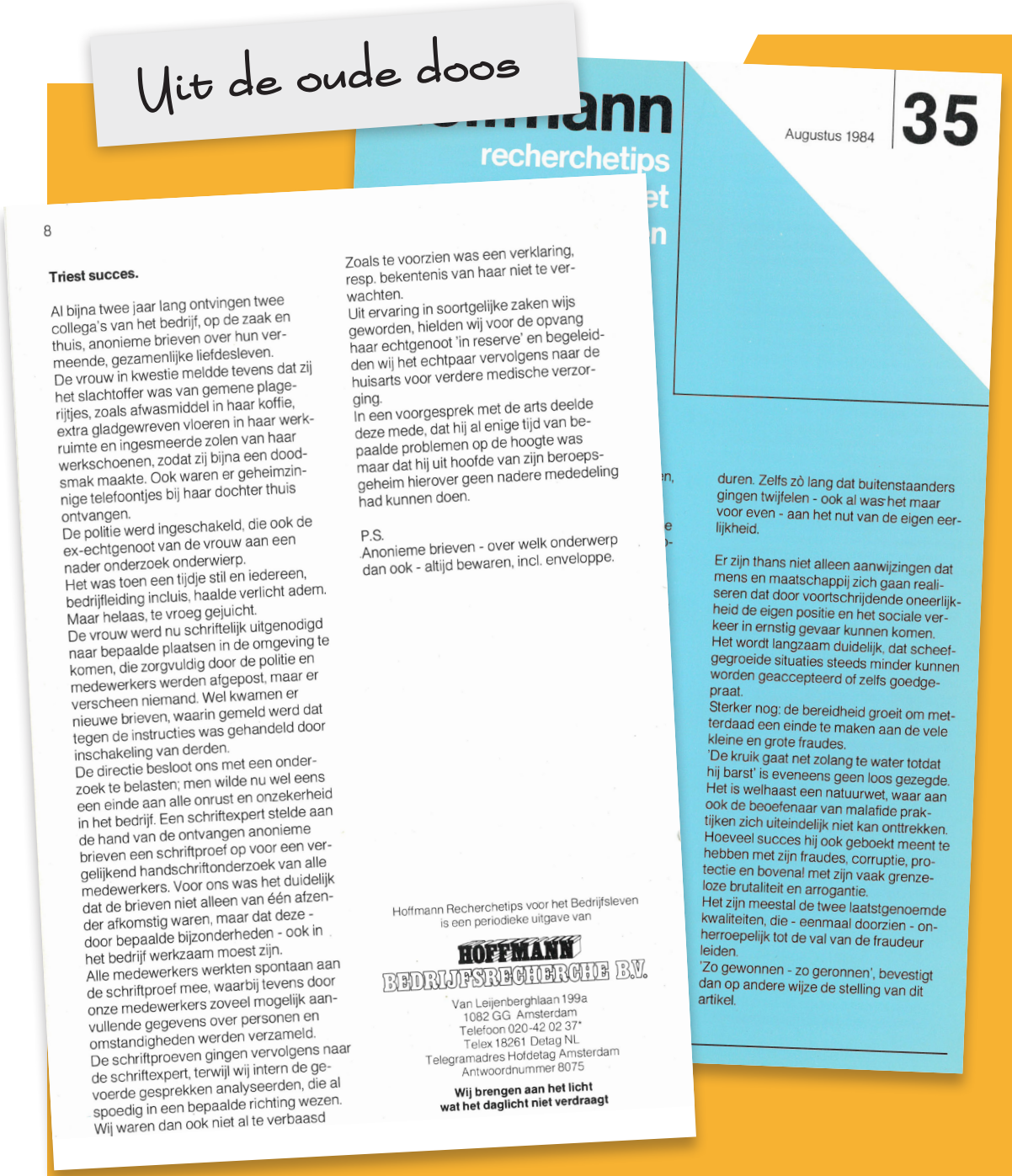
Nu is de digitalisering van de samenleving nog volop in ontwikkeling. Veel bedrijven zijn daarin al heel ver, andere organisaties moeten nog een flinke stap maken. Ook in de beveiliging van hun data en systemen. Welke ontwikkelingen signaleert Joost op dit moment, naast de toename in ransomware aanvallen? Joost: "Waar organisaties vroeger vaak een server 'on premise' hadden, ervaren we tegenwoordig dat steeds meer organisaties hun data en systemen naar de Cloud brengen. Dat is enerzijds begrijpelijk, maar anderzijds ook een uitdaging voor ons als onderzoeker, aangezien relevante onderzoeksdata minder beschikbaar wordt. Daarnaast zie je dat enkele organisaties nog geen gebruik maken van twee factor authenticatie, waardoor onbevoegden met de juiste inloggegevens bij de data kan.

"Daarnaast merken we dat digitaal onderzoek steeds uitdagender wordt," vervolgt Joost. "Dat heeft verschillende oorzaken. Een oorzaak is bijvoorbeeld de invoering van de AVG. Omwille van de privacy wordt steeds meer onderzoeksinformatie afgeschermd. Denk bijvoorbeeld aan gegevens van een eigenaar die een domeinnaam heeft geregistreerd of het loggen van IP-adressen. Dat maakt de uitdaging voor ons groter, we moeten nog slimmer gaan werken."

Een andere oorzaak die Joost noemt is de beperkte beschikbaarheid van loggegevens. Joost: "Hoe meer loggegevens er beschikbaar zijn, hoe meer wij kunnen onderzoeken. Maar vaak is de standaard bewaartijd van logbestanden maar 30 dagen, terwijl een incident verder in het verleden heeft plaatsgevonden. Ook zien we een groei van virtuele gebruikersprofielen, zoals het gebruik van Citrix omgevingen. Vaak worden virtuele gebruikersprofielen om de zoveel tijd gereset. Daarmee gaat helaas relevante onderzoeksdata verloren."

Wat kunnen organisaties doen om te zorgen dat digitaal forensisch onderzoekers hun werk goed kunnen doen, op het moment dat er iets gebeurt? Joost: "Het is belangrijk dat organisaties werk maken van hun forensic readiness. We zien vaak dat zij zich onvoldoende bewust zijn van de risico's en er dus ook onvoldoende budget voor uittrekken. Totdat zich een incident voordoet en digitaal onderzoek minder goed mogelijk blijkt. Dan slaan zij zichzelf voor hun kop. Concreet zou ik organisaties dus willen adviseren om de bewaartijden van hun logbestanden te verhogen, tot 90 dagen bijvoorbeeld. Maar ook om de gebruikersprofielen van medewerkers langer te bewaren en goede back-ups te maken van digitale data. Daarnaast is het goed als organisaties in gesprek gaan met hun medewerkers. Medewerkers bewust laten worden van digitale dreiging. Welke informatie zetten medewerkers bijvoorbeeld op social media en waar kleven risico's aan voor de organisatie? Hoe gaan ze om met e-mailberichten en vertrouwelijke informatie? Hoe is de thuiswerkplek beveiligd? Dat soort zaken."

Uit de oude doos



8

Triest succes.

Al bijna twee jaar lang ontvingen twee collega's van het bedrijf, op de zaak en thuis, anonieme brieven over hun vermeende, gezamenlijke liefdesleven.
De vrouw in kwestie meldde tevens dat zij het slachtoffer was van gemene plagerijtjes, zoals afwasmiddel in haar koffie, extra gladgewreven vloeren in haar werkruimte en ingesmeerde zolen van haar werkschoenen, zodat zij bijna een doodsmak maakte. Ook waren er geheimzinnige telefoontjes bij haar dochter thuis ontvangen.
De politie werd ingeschakeld, die ook de ex-echtgenoot van de vrouw aan een nader onderzoek onderwierp.
Het was toen een tijdje stil en iedereen, bedrijfleiding incluis, haalde verlicht adem.
Maar helaas, te vroeg gejuicht.
De vrouw werd nu schriftelijk uitgenodigd naar bepaalde plaatsen in de omgeving te komen, die zorgvuldig door de politie en medewerkers werden afgepost, maar er verscheen niemand. Wel kwamen er nieuwe brieven, waarin gemeld werd dat tegen de instructies was gehandeld door inschakeling van derden.
De directie besloot ons met een onderzoek te belasten; men wilde nu wel eens een einde aan alle onrust en onzekerheid in het bedrijf. Een schriftexpert stelde aan de hand van de ontvangen anonieme brieven een schriftproef op voor een vergelijkend handschriftonderzoek van alle medewerkers. Voor ons was het duidelijk dat de brieven niet alleen van één afzender afkomstig waren, maar dat deze - door bepaalde bijzonderheden - ook in het bedrijf werkzaam moest zijn.
Alle medewerkers werkten spontaan aan de schriftproef mee, waarbij tevens door onze medewerkers zoveel mogelijk aanvullende gegevens over personen en omstandigheden werden verzameld.
De schriftproeven gingen vervolgens naar de schriftexpert, terwijl wij intern de gevoerde gesprekken analyseerden, die al spoedig in een bepaalde richting wezen.
Wij waren dan ook niet al te verbaasd

Zoals te voorzien was een verklaring, resp. bekentenis van haar niet te verwachten.
Uit ervaring in soortgelijke zaken wijs geworden, hielden wij voor de opvang haar echtgenoot 'in reserve' en begeleidden wij het echtpaar vervolgens naar de huisarts voor verdere medische verzorging.
In een voorgesprek met de arts deelde deze mede, dat hij al enige tijd van bepaalde problemen op de hoogte was maar dat hij uit hoofde van zijn beroepsgeheim hierover geen nadere mededeling had kunnen doen.

P.S.
Anonieme brieven - over welk onderwerp dan ook - altijd bewaren, incl. enveloppe.

Hoffmann Recherchetips voor het Bedrijfsleven
is een periodieke uitgave van

HOFFMANN
BEDRIJFSRECHERCHE B.V.

Van Leijenberghlaan 199a
1082 GG Amsterdam
Telefoon 020-42 02 37*
Telex 18261 Detag NL
Telegramadres Hofdetag Amsterdam
Antwoordnummer 8075

Wij brengen aan het licht
wat het daglicht niet verdraagt

recherchetips

Augustus 1984 **35**

duren. Zelfs zò lang dat buitenstaanders gingen twijfelen - ook al was het maar voor even - aan het nut van de eigen eerlijkheid.

Er zijn thans niet alleen aanwijzingen dat mens en maatschappij zich gaan realiseren dat door voortschrijdende oneerlijkheid de eigen positie en het sociale verkeer in ernstig gevaar kunnen komen.
Het wordt langzaam duidelijk, dat scheefgegroeide situaties steeds minder kunnen worden geaccepteerd of zelfs goedgepraat.
Sterker nog: de bereidheid groeit om metterdaad een einde te maken aan de vele kleine en grote fraudes.
'De kruik gaat net zolang te water totdat hij barst' is eveneens geen loos gezegde.
Het is welhaast een natuurwet, waar aan ook de beoefenaar van malafide praktijken zich uiteindelijk niet kan onttrekken.
Hoeveel succes hij ook geboekt meent te hebben met zijn fraudes, corruptie, protectie en bovenal met zijn vaak grenzeloze brutaliteit en arrogantie.
Het zijn meestal de twee laatstgenoemde kwaliteiten, die - eenmaal doorzien - onherroepelijk tot de val van de fraudeur leiden.
'Zo gewonnen - zo geronnen', bevestigt dan op andere wijze de stelling van dit artikel.

Deze casus 'Triest succes' is gepubliceerd in de 'Recherche Tips van augustus 1984'.

"Hoffmann, jullie doen toch alleen fraude onderzoeken?"

Sinds de MeToo beweging in 2017 is er een enorme toename zichtbaar in onderzoeken naar grensoverschrijdend gedrag op de werkvloer. Dat is bij Hoffmann niet anders. Zeker nadat een aantal grote organisaties in de media kwam begin dit jaar, stroomden de telefoontjes binnen. Regelmatig wordt er naar grensoverschrijdend gedrag gekeken als iets van deze tijd, een verandering in cultuur en tolerantie. Toch is het helaas iets van alle tijden en het doen van onderzoek hiernaar is voor Hoffmann geen onbekend terrein. Al 60 jaar schakelen bedrijven Hoffmann in voor integriteitsonderzoeken. De boodschap uit 1984 luidt anno 2022 nog steeds: Sta op, neem maatregelen en voorkom grensoverschrijdend gedrag!

Tara – onderzoeker Fraude & Integriteit bij Hoffmann

Er valt *altijd* iets te regelen ...

Bij een woningbouwvereniging in Nederland kwam een melding binnen van een potentiële huurder. Hij had een woning 's avonds, buiten werktijd, bezichtigd. En de woonconsulent had gevraagd of hij iets extra's voor de woning wilde betalen. Natuurlijk sprak de woningbouwvereniging haar medewerker daarop aan. Maar die ontkende dat er over geld gesproken was. Een paar maanden later staat er iemand aan de balie. De vraag van deze huurder: wanneer kan ik in mijn nieuwe woning? Het antwoord: je kan er helemaal nog niet in, want deze woning staat nog niet te huur. De zogenaamde huurder baalt, want ze had al wel voor de woning betaald. Beide incidenten wijzen in de richting van dezelfde persoon. Reden genoeg voor de directie om ons in te schakelen voor een onderzoek.

Een duik in het papierwerk
De medewerker wordt vrijgesteld van werk en wij krijgen toegang tot al zijn dossiers en administratie. Opvallend is dat de administratie mankementen vertoont. Zo missen er ondertekende verklaringen en documenten die aangeven dat huurders voldoen aan inkomenseisen. Ook zien we dat een aantal woningen extreem snel zijn verhuurd nadat de woning online kwam. Eigenlijk onmogelijk, want normaal is er zeker een week nodig voor bezichtigingen en het papierwerk. Onze duik in de administratie levert dus een hoop rook en vraagtekens op.

Een duik in de zakelijke telefoon
We lezen ook de zakelijke telefoon van de medewerker uit. Daarbij komen we WhatsApp-gesprekken tegen die verdacht zijn. Maar geen concrete bewijzen. Dan vinden we een voicemail van een bekende van de medewerker. Of hij nog huizen in twee andere woonplaatsen kan regelen. De woonplaatsen die genoemd worden, zijn de plaatsen waar deze woonconsulent eerder heeft gewerkt. Dat zien we terug op zijn cv.

Gesprek met de woonconsulent
Natuurlijk confronteren wij de betreffende woonconsulent met onze bevindingen. Met de hiaten in de administratie, de onrealistische tijdspaden en de berichten op zijn telefoon. De woonconsulent ontkent alles. Er is niets waar van onze bevindingen. Terwijl we in gesprek zijn, denkt één van onze onderzoekers hem te herkennen. Ook dat ontkent de woonconsulent. Na een snelle zoekopdracht in onze eigen dossiers blijkt echter dat hij al eerder bij ons aan tafel heeft gezeten in het verleden. Bij een andere woningbouwvereniging werd hij toen verdacht van frauduleuze handelingen. De woonconsulent wil daar niets over zeggen tijdens ons gesprek.

Ontslagen en vertrokken
De woonconsulent wordt ontslagen door onze opdrachtgever. Bijzonder is dat hij zijn ontslag niet aanvecht. Met de staart tussen de benen vertrekt hij bij de woningbouwvereniging. Deze casus leidt er vervolgens toe dat de woningbouwvereniging haar screeningsproces nog verder verbetert. Om beter te weten wie ze in huis haalt!

Hoffmann

Vertrouwen is goed,

Hoffmann is beter

Over Hoffmann
Uw veiligheid, daar maken we ons sterk voor, al bijna 60 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.

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. 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