HOFFMANN TIPS

voor bedrijfsleven en publieke sector

#237 | mei 2019

Uw belang is waarheidsvinding

Spoofing?
Wie heb ik aan de lijn?

De Wet bescherming bedrijfsgeheimen

Declareren kun je leren

Genadeloos testen op informatiebeveiliging

Hoffmann

Column

Uw belang is waarheidsvinding

Integriteit is ons handelsmerk, dáár staan we voor, ook als merk. Integriteit kost ons eigenlijk ook geen enkele moeite, totdat … de integriteit van Hoffmann in een bepaalde zaak publiekelijk ter discussie wordt gesteld. Dan voel je de onmacht en jeuken je handen om het dossier erbij te pakken en te laten zien wat er daadwerkelijk is gebeurd.

Het uitschakelen van deze emotie hoort ook bij ons vak. En dat kost soms wat moeite, maar het klantbelang staat altijd voorop. Met onze belofte *Vertrouwen is goed Hoffmann is beter*, mag dat ook van ons verwacht worden.

Als oudste en grootste onderzoeksbureau van Nederland hebben we een goede naam en staan we bekend als betrouwbare partner. Wij doen aan waarheidsvinding en zien onszelf als de onpartijdige feitenonderzoeker die feiten onderzoekt en rapporteert. Ik ben er namelijk van overtuigd dat we alleen in die rol meerwaarde kunnen bieden. Alleen dan krijgt onze klant een rapport dat op waarheid en feiten is gebaseerd en bepaalde overtuigingskracht heeft. Ook wanneer u als onze klant liever iets anders had willen zien of horen. Wij zijn geen partij in het conflict. Onze doelstelling is om op een integere en objectieve manier de feiten vast te stellen. Het is vervolgens aan u om (eventueel met een jurist) conclusies te trekken op basis van onze bevindingen.

En toch is het best logisch dat we onbedoeld betrokken raken in een zaak. Ons werk vindt vaak plaats op het moment dat er sprake is van een (potentieel) conflict. Bijvoorbeeld tussen twee zakenpartners. Tussen werkgever en werknemer. Of tussen een leverancier en zijn klant. Er bestaat een verdenking of er is onenigheid over gebeurtenissen.

En hoewel we dat niet willen, blijkt in de praktijk dat we juist daarom betrokken kunnen raken in dat conflict. Misschien vraagt u zich af: *waarom is dat erg?* Omdat we onpartijdig willen zijn en blijven. We onthouden ons van een oordeel en opereren altijd binnen de wettelijke kaders. Dit betekent ook, en dat gebeurt regelmatig, dat we opdrachten om die reden moeten weigeren. En dat doen we, omdat we onze professionele en onpartijdige rol heel serieus nemen.

Ook u krijgt misschien wel te maken met tegenwind. Een medewerker die uw bedrijf schade toe brengt. Buitenstaanders die uw bedrijf en systemen binnen proberen te komen.
Hoe kunt u zich voorbereiden op die tegenwind? In deze Tips hebben we weer een aantal interessante artikelen voor u verzameld.

Ik wens u veel leesplezier!

MARTIJN VAN DE BEEK

Een eigen handeltje tijdens ziekte

Onze opdrachtgever in de koffiebranche heeft een zieke medewerker in dienst. Hij kan zijn werkzaamheden als servicemonteur niet meer uitvoeren. Onder andere omdat hij niet in staat is om lang auto te rijden en te tillen. Maar dan komt er een mail binnen. Op basis daarvan vraagt de werkgever zich af of de zieke medewerker zonder toestemming een eigen handeltje is begonnen. En voert hij werkzaamheden uit die hij zegt niet te kunnen uitvoeren? De opdrachtgever schakelt ons in om de situatie te onderzoeken.

Observaties met proefaankoop
Naast observaties zetten we een proefaankoop in als opsporingsmethode in deze zaak. We reageren op een advertentie waarin de zieke medewerker onder een valse naam een koffiemachine aanbiedt. De koop vindt plaats bij een groot winkelcomplex, want de medewerker moet daar toch zijn om een nieuw bankstel te kopen. Op de dag van de koop zien we hem inderdaad in een auto met aanhangwagen arriveren. Later maken we foto's van hoe hij het nieuwe bankstel samen met zijn vriendin in de aanhanger tilt.

Reparatie nodig
De zieke medewerker geeft ons zijn visitekaartje en vertelt dat hij ook koffiemachines repareert. Na een tijdje nemen we daarover contact met hem op. Onze opdrachtgever heeft ons een kapot apparaat ter beschikking gesteld die we bij de medewerker thuis brengen. Daar helpt hij ons met uitladen en gaat hij ons voor naar zijn werkplaats vol gereedschap, onderdelen en een aantal koffiemachines. Na afloop van de reparatie krijgen we een professionele factuur.

Het vervolg
Normaal confronteren onze rechercheurs de medewerker met de bevindingen. Zij zijn onafhankelijk en zijn ervaren in de opbouw van zo'n confronterend gesprek. Maar ondanks ons advies wilde de werkgever toch zelf de confrontatie aan gaan.
De medewerker ontkent echter koffiemachines te verkopen en te repareren. Maar op basis van de feiten ontbindt de rechter uiteindelijk de arbeidsovereenkomst. Ook moet de medewerker de kosten van ons onderzoek terugbetalen aan de opdrachtgever.

Hoffmann ontvangt ISO/IEC 27001:2013 certificaat van DEKRA

Hoffmann heeft als recherchebureau te maken met strenge regels op het gebied van privacy, waardoor de beveiligingsmaatregelen op het gebied van informatiebeveiliging streng worden gehanteerd. Hoffmann werkt al jaren volgens de ISO27001 norm en heeft zich daar eind 2018 op laten auditen. Op 27 december heeft de organisatie formeel voor al haar afdelingen; Cybersecurity-Riskmanagement-Recherche, de ISO 27001 certificering ontvangen.


CERTIFICAAT
DEKRA
Hoffmann Bedrijfsrecherche B.V.
ISO/IEC 27001:2013

Het certificaat toont aan dat Hoffmann voldoet aan de normen van de internationale standaard en beschikt over een duidelijk beleid rondom data en informatiebeveiliging. Dit betekent o.a. dat Hoffmann op een verantwoordelijke manier omgaat met vertrouwelijke informatie. Een belangrijke erkenning richting de medewerkers en de uitgebreide klantenkring. Maarten IJzermans, Director Riskmanagement van Hoffmann, benoemd deze formele certificering; "een bevestiging van het hoge beveiligingsniveau van de organisatie."

De certificering is uitgevoerd door DEKRA, één van de grootste test- en certificatie-instellingen ter wereld. DEKRA heeft uitgebreide expertise in het auditen en certificeren van managementsystemen op het gebied van kwaliteit, veiligheid, duurzaamheid en informatiebeveiliging.


Wat is dat nu weer
en hoe weet ik zeker
wie ik aan de lijn heb?
Spoofing?

"'Goedemiddag, u spreekt met de servicedesk'. Het nummer op mijn display laat inderdaad het nummer van de servicedesk zien. 'Er is iets mis met uw e-mail account. Kunnen wij samen de instellingen nalopen ? Kunt u voor mij naar de volgende website gaan of uw gebruikersnaam en wachtwoord geven ter verificatie?' Achteraf klinkt het zo logisch dat ik deze gegevens nooit via de telefoon had moeten afgeven, maar ik geloofde echt dat ik de servicedesk aan de lijn had. En ik wilde echt geen problemen met mijn e-mail account!"

Een voorbeeld uit onze dagelijkse praktijk. Het afgelopen jaar gaf 70% van de door ons geteste medewerkers van onze klanten hun loginnaam en wachtwoord af via de telefoon. Een techniek die voice-phishing (vhishing) wordt genoemd en waar wij onze klanten bewust van maken en mee helpen om zo te voorkomen dat gevoelige informatie in verkeerde handen komt.

Maar een tweede techniek maakt het ineens nog veel moeilijker om kwaadwillenden buiten de deur te houden: Caller ID spoofing. Met caller ID spoofing doet iemand zich voor als een ander, door te bellen met een eigen telefoon, terwijl het telefoon-nummer van een ander op het display verschijnt.

Deze techniek is al langer bekend en wordt vaak op een legale manier door bedrijven gebruikt, bijvoorbeeld om de doorkiesnummers van medewerkers af te schermen. Zij sturen dan alleen het algemene telefoonnummer mee. Een goede manier om de gewenste informatie bij de klant te krijgen.

Caller ID spoofing is extreem eenvoudig toe te passen. Er zijn meerdere websites die deze dienst aanbieden. Op deze websites wordt de dienst gepromoot voor privé ("Houd je familie en vrienden voor de gek!") en zakelijke ("Uw klanten zien alleen uw zakelijke nummer") doeleinden. Maar juist omdat het zo eenvoudig is, wordt er ook misbruik van gemaakt.

Fraudeurs kunnen hierdoor eenvoudig een valse hoedanigheid aannemen (Artikel 326 Wetboek van Strafrecht). Met caller ID spoofing kunt u zich voor doen als iemand anders, zoals bijvoorbeeld: een systeem-beheerder, servicedeskmedewerker, leverancier, bankier, accountant of - in grote bedrijven - de directeur. En uw medewerkers kunnen door het zien van het "juiste" telefoonnummer op het verkeerde been worden gezet.

De fraudeur kan dan tijdens het telefoongesprek informatie proberen te verkrijgen zoals:

- Gebruikersnamen en wachtwoorden van uw medewerkers, indien mogelijk accounts resetten bij de servicedesk, om zo uw netwerk binnen te kunnen dringen.
- Privacygevoelige persoonsgegevens, zoals BSN-nummers, rekeningnummers en adresgegevens.
- Vertrouwelijke informatie, bijvoorbeeld over patenten of andere bedrijfsgeheimen.

Omdat u denkt dat u een collega, relatie of leverancier aan de telefoon hebt, kan het zijn dat u gevraagd wordt een rekeningnummer te wijzigen, bestanden te wijzigen. Geldbedragen over te maken namens de directie. Deze laatste vorm van fraude wordt ook wel CEO-fraude genoemd. Het kan hierbij gaan om flinke bedragen.

Wat kunt u doen?

Natuurlijk ligt hier een taak voor de overheid en telecomproviders. De overheid zou maatregelen moeten nemen om het spoofen van telefoonnummers tegen te gaan. Daarnaast zouden telecomproviders maatregelen kunnen nemen om dit soort telefoontjes te blokkeren.

Omdat het in Nederland nog niet zover is, delen wij hier de vier belangrijkste tips om te voorkomen dat uw bedrijf schade lijdt door caller ID spoofing en voice-phishing:

- Zorg dat uw medewerkers zich bewust zijn van dit gevaar.
- Spreek met uw medewerkers af dat zij in een inkomend telefoongesprek nooit persoonlijke en/of vertrouwelijke informatie verstrekken. Laat ze in plaats daarvan vragen of ze op een later moment kunnen terugbellen.
- Spreek met uw medewerkers af dat zij nooit telefonisch betalingsopdrachten aannemen. Van wie dan ook, ook niet van de CEO of CFO.
- Maak goede afspraken met externe leveranciers over telefonische communicatie. Spreek bijvoorbeeld met hen af dat er nooit telefonisch over inloggegevens en wachtwoorden zal worden gecommuniceerd.

Bedrijfsspionage

Hoe beperk je de impact?

Het meenemen van vertrouwelijke bedrijfsgegevens van chipmachinemaker ASML door oud-medewerkers naar concurrent XTAL heeft de aandacht voor bedrijfsspionage vergroot. Hoewel bedrijfsspionage niet volledig uit te bannen is, kunnen betrekkelijk simpele maatregelen de eventuele gevolgen wel beperken.

#1

Medewerkers dienen zich bewust te zijn van het risico dat bedrijfsspionage kan plaatsvinden. Middelen of processen die – op welke wijze dan ook – voor andere organisaties van belang kunnen zijn, zijn potentiële doelwitten. Het kan gaan om concurrenten die interesse hebben in bedrijfsprocessen of nieuw ontwikkelde producten, maar ook om werknemers die klantgegevens meenemen voor hun eigen startup. Bewustzijn dat dergelijke vertrouwelijke informatie kwetsbaar is, leidt tot alertheid onder medewerkers met betrekking tot verdachte situaties en vormt de basis voor de onderstaande maatregelen.

#2

Vertrouwelijke informatie hoort slechts beschikbaar te zijn voor medewerkers die daadwerkelijk met die informatie moeten werken. Medewerkers of externen die de vertrouwelijke informatie niet nodig hebben voor hun dagelijkse werkzaamheden, krijgen geen toegang tot die vertrouwelijke informatie. Dit zogeheten need-to-know-principe uit zich in de afscherming van fysieke en digitale locaties waar de vertrouwelijke informatie zich bevindt; alleen geautoriseerde medewerkers kunnen daar bij. Geautoriseerde medewerkers begeleiden continu ongeautoriseerde medewerkers of externen zodra die incidenteel toegang tot vertrouwelijke informatie nodig hebben. Daarbij dienen ook controles plaats te vinden of op de locaties van vertrouwelijke informatie items zijn ontvreemd of achtergelaten, in het bijzonder gegevensdragers of sensoren.

#3

Voordat een bedrijf een medewerker kan autoriseren om toegang te krijgen tot de vertrouwelijke informatie, dient het bedrijf te verifiëren dat de medewerker betrouwbaar is. Idealiter gebeurt dit door middel van een screening. Bij een screening vindt controle plaats van de identiteit van de medewerker en is aandacht voor de achtergrond van de medewerker. De achtergrondcheck dient om te beoordelen of omstandigheden of eerdere gedragingen van de (kandidaat-) medewerker een risico vormen in relatie tot de vertrouwelijke informatie. Een bedrijf dient zich bewust te zijn van een mogelijk risico op bedrijfsspionage als het bijvoorbeeld iemand aanneemt die via vrienden of familie nauwe banden onderhoudt met een concurrerend bedrijf. Een screening maakt dergelijke risico's inzichtelijk, op basis waarvan het bedrijf kan besluiten iemand al dan niet toegang tot vertrouwelijke informatie te geven. Omstandigheden van medewerkers kunnen wijzigen, ook na een screening. Daarom is het van belang screeningen van medewerkers die toegang hebben tot vertrouwelijke informatie periodiek te herhalen.

Integrity Due Diligence: weet met wie u zaken doet

Als u een zakelijke relatie aangaat wilt u natuurlijk precies weten met wie u zaken gaat doen. Wie zitten er achter deze partij? Hoe (integer) doen zij zaken? Hebben zij een goede reputatie? Houden ze zich aan (inter)nationale regels op het gebied van omkoping, anti-corruptie en mensenrechten? Een Integrity Due Diligence geeft antwoord op de vraag welke integriteitsrisico's u loopt door met deze partij in zee te gaan.

De aanpak van Hoffmann onderscheidt zich daarbij door onze focus op de bestuurders achter het bedrijf. Veel andere Third Party Due Diligence-onderzoeken richten zich, via boekenonderzoek, met name op financiële, fiscale, juridische en commerciële aspecten. Hoffmann analyseert de integriteit van de bestuurder niet alleen door middel van screening en een open bronnen-onderzoek, maar ook door persoonlijke gesprekken, met de bestuurder zelf én met referenten. De bestuurder moet daaraan wel willen meewerken, maar volgens ons is dit de enige betrouwbare manier om integriteitsrisico's echt goed in kaart te brengen.

Zicht op uw zakenpartner(s)
Een Integrity Due Diligence is onmisbaar als u zakelijke relaties van enige omvang aangaat. Na een Integrity Due Diligence-onderzoek bent u zich bewust van de integriteitsrisico's en kunt u een weloverwogen beslissing nemen. Daarmee voorkomt u reputatieschade, onverwachte kosten (bijvoorbeeld door boetes) en uitsluiting van opdrachten.

Wat is Integrity Due Diligence?
Integrity Due Diligence wordt ook wel Third Party Due Diligence genoemd. Een Integrity Due Diligence-onderzoek identificeert risico's die niet zichtbaar worden in andere due diligence-onderzoeken, omdat het zich richt op de integriteitsrisico's van partijen waar u zaken mee wilt gaan doen. Denk daarbij aan:

- fusie- of overnamekandidaten
- fabrikanten
- leveranciers
- franchisenemers, distributeurs of agenten
- zakelijke partners en relaties

Wat houdt een Integrity Due Diligence in?
De aard, inhoud en diepgang van de onderzoekshandelingen binnen een Integrity Due Diligence verschillen, maar moeten altijd in verhouding staan tot de in verband met het zakelijke belang te beheersen integriteitsrisico's. Mogelijke onderzoekshandelingen zijn:

- onderzoek naar de integriteit van de bestuurder(s) en/of de UBO (Ultimate Benificial Owner)
- controle op maatschappelijk verantwoord ondernemen
- controle op compliance
- onderzoek naar corruptie en omkoping

De Wet bescherming bedrijfsgeheimen

Op 23 oktober 2018 is de Wet bescherming bedrijfsgeheimen (Wbb) in werking getreden. Daarmee worden bedrijfsgeheimen voor het eerst ook wettelijk beschermd. In de Wbb is vastgelegd wat er onder een bedrijfsgeheim wordt verstaan en hoe u tegen inbreuken kunt optreden.

Wat is een bedrijfsgeheim?
Een bedrijfsgeheim kan zich richten op formules of recepten, werkprocessen, technische kennis of software, maar ook op concepten, een strategie, onderzoeksgegevens of een klantenbestand. De Wbb definieert een bedrijfsgeheim als informatie:

- die geheim is in die zin dat zij niet algemeen bekend of gemakkelijk toegankelijk is voor de personen die zich met dit soort informatie bezig houden;
- die handelswaarde bezit omdat zij geheim is; en
- waarbij redelijke maatregelen zijn genomen om de informatie geheim te houden.

Alleen als aan al deze drie voorwaarden is voldaan kunt u zich beroepen op de Wbb.

Hoe kunt u inbreuken voorkomen?
Als u bedrijfsgeheimen heeft moet u dus redelijke maatregelen nemen om de informatie geheim te houden. Dit kunnen zowel technische als contractuele maatregelen zijn. Denkt u daarbij aan:

- Fysieke beveiliging van uw bedrijf en informatie, door middel van een alarm, bewakingscamera's, toegangsprotocollen en een kluis.
- Digitale beveiliging van uw informatie met wachtwoorden, encryptie, beveiligingssoftware of een digitale kluis.
- Concurrentiebedingen, geheimhoudingsclausules en intellectueel eigendomsbedingen in uw arbeidsovereenkomsten en personeelshandboeken.
- Geheimhoudingsclausules in de overeenkomsten met uw zakenpartners.

Worden uw bedrijfsgeheimen bekend omdat u geen of onvoldoende redelijke maatregelen had genomen? Dan kunt u geen beroep doen op de Wbb.

Wat kunt u doen tegen inbreuken?
Er is sprake van een inbreuk op uw bedrijfsgeheim als iemand het bedrijfsgeheim onrechtmatig heeft verkregen, gebruikt of openbaar heeft gemaakt. Op grond van de Wbb kunt u de rechter dan vragen:

- te verbieden dat de ander uw bedrijfsgeheim openbaar maakt;
- te verbieden dat de ander inbreukmakende producten produceert of op de markt brengt;
- beslag te mogen leggen op inbreukmakende producten;
- inbreukmakende producten terug te mogen roepen, uit de handel te mogen nemen of te mogen vernietigen;
- de ander te veroordelen tot een schadevergoeding;
- de ander te veroordelen tot openbaarmaking van de rechterlijke uitspraak.

Wilt u meer weten? Neem contact met ons op en onze experts beantwoorden graag uw vragen.

Internationale onderzoeken

De vele fraude onderzoeken brengen onze bedrijfsrechercheurs vaak buiten de grenzen van Nederland. Veel fraudebendes, vooral als het om online fraude gaat, opereren vanuit het buitenland. Maar niet alleen de dader brengt ons naar het buitenland. Veel grote organisaties waar we voor werken hebben vestigingen in Europa of elders in de wereld.

Dankzij deze internationale onderzoeken hebben we veel contacten in de betreffende landen opgebouwd waardoor de onderzoeken alleen maar efficiënter worden. Wij maken ook veelvuldig gebruik van ons wereldwijd partnernetwerk aangezien wet- en regelgeving per land kan verschillen. De dienstverlening is niet anders dan in Nederland. Al onze mogelijke diensten van integriteitsonderzoeken tot observaties, van verborgen camera tot digitale onderzoeken kunnen overal plaatsvinden. Voor preventieve onderzoeken geldt hetzelfde. We kunnen medewerkers screenen, inlooptesten doen (red teaming) of we kunnen een inventarisatie maken om de risico's van het bedrijf in kaart te brengen. Rekening houdend met de wettelijke kaders van het betreffende land gaan we graag voor u aan de slag.

Casus

Genadeloos testen op informatiebeveiliging

Vanaf 2020 vervangt de Baseline Informatiebeveiliging Overheid (BIO) de Baseline Informatiebeveiliging Gemeenten (BIG) en geldt dan breder voor overheden. Informatiebeveiliging is een hot topic en staat bij veel rekenkamercommissies op de agenda om te onderzoeken. Vanwege het specialistische karakter van het onderzoek schakelen zij Hoffmann dan bij. Afgelopen jaar voerden we in opdracht verschillende onderzoeken uit bij gemeentes waar de hoofdvraag luidde: Wat is de stand van zaken op het gebied van informatiebeveiliging?

Hacken vanaf het internet en het interne netwerk

In onze onderzoeken was vaak de vraag of de informatiesystemen van de gemeente voldoende beschermd zijn tegen het risico van hacken, lukt het ons om via internet en zonder enige kennis vanuit de organisatie binnen te komen in de ict-systemen? Nee, dat lukte niet altijd. Toch vonden we wel systemen die niet voorzien waren van alle beveiligingsupdates. Een risico waar hackers met meer tijd ongetwijfeld gebruik van hadden gemaakt.

Voice phishing

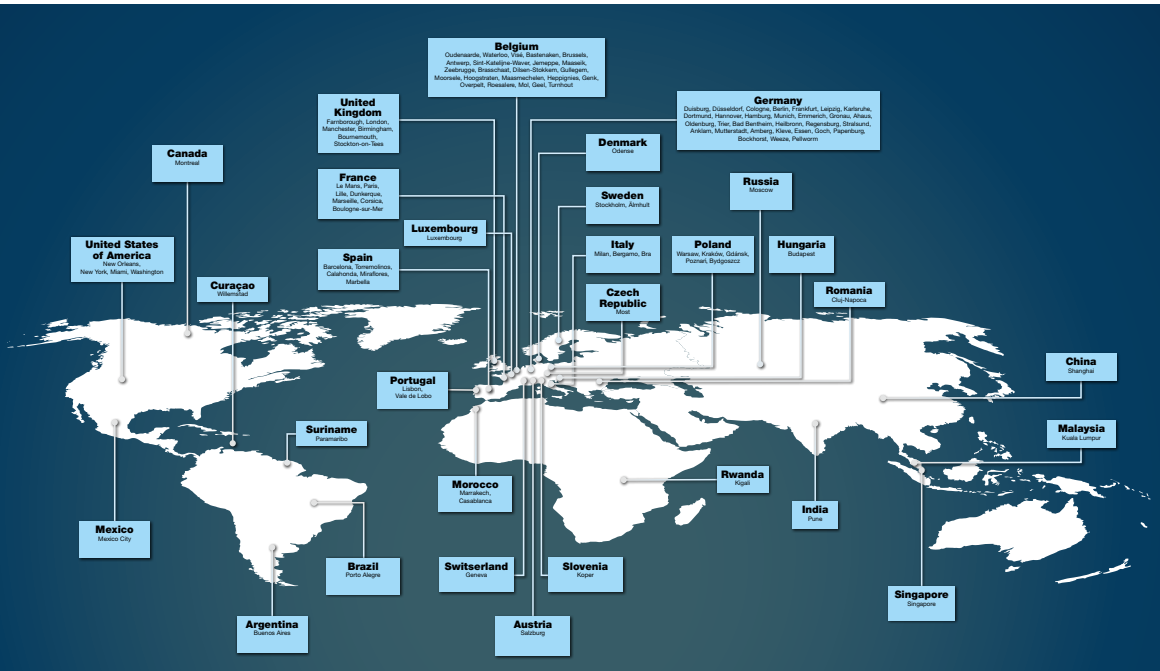
De volgende vraag: hoe ver kunnen we binnendringen als we inloggegevens hebben? Om die gegevens te bemachtigen, belden wij een aantal medewerkers op. In het telefoongesprek deden we ons voor als iemand van de servicedesk. Een geloofwaardig verhaal en een bekend telefoonnummer? Dan ben je al snel geneigd om te klikken op een link die de beller stuurt. Onze missie was geslaagd. Met de inloggegevens konden wij vervolgens binnendringen in de ict-systemen van de gemeente. Het risico daarvan? Een kwaadwillende zou alle systemen plat kunnen leggen of zich toegang kunnen verschaffen tot vertrouwelijke informatie.

Netjes binnenlopen

Hoe gaan medewerkers met een vreemde op de werkvloer om? Dit keer ging één van onze medewerkers keurig in pak naar binnen. Onze medewerker had geen pasje, maar die heb je ook niet nodig als de deur open staat … En als je je handen vol hebt, is er altijd wel iemand zo vriendelijk om de deur even open te houden. Niemand stelde vragen. Zo kon onze medewerker toegang krijgen tot archiefkasten en had hij zelfs een laptop mee kunnen nemen.

Met het oog op de toekomst

Natuurlijk was het niet altijd leuk om de bevindingen en de conclusies uit ons onderzoek te lezen. Toch werden de aanbevelingen uit ons onderzoek heel serieus opgepakt. In veel gevallen leiden onze aanbevelingen tot verbeterplannen. Ook zien we dat gemeentes blij zijn met het inzicht wat we ze kunnen verschaffen. Zo worden wij in navolging op het onderzoek van de rekenkamercommissie gevraagd om periodiek te testen en kwetsbaarheden in kaart te brengen. Zo nemen gemeentes serieuze stappen met het oog op de toekomst.



Bijdrage van onze partner Capra advocaten, door J.J. Blanken

Declareren kun je leren

Per 1 januari 2020 wordt de rechtspositie van de meeste ambtenaren fors gewijzigd. Weliswaar blijft de ambtelijke status bestaan, doch ten gevolge van de Wet normalisering rechtspositie ambtenaren (Wnra) zijn er zeer veel wijzigingen op komst, zowel wat betreft de toepasselijke wettelijke regelingen als de arbeidsvoorwaarderegelingen en het procesrecht.

Wat niet verandert, is dat strenge integriteitsregels gelden bij overheid, onderwijs en zorg. Zowel onder de oude als de nieuwe Ambtenarenwet geldt een verplichting voor overheden om een integriteitsbeleid te voeren en regels ter zake vast te stellen. Die regels gelden voor ambtenaren, bestuurders en (andere) politiek ambtsdragers. Voor de ambtenaren is van belang dat zij na 1 januari 2020 met een andere rechter worden geconfronteerd, namelijk de civiele rechter in plaats van de bestuursrechter. Als we de bestaande jurisprudentie van beide rechters vergelijken, dan valt op dat de benadering behoorlijk kan verschillen. Het lijkt er soms op dat de civiele rechter ervan uitgaat dat een werknemer alles mag wat niet expliciet is verboden en dat de bestuursrechter uitgaat van de benadering dat een ambtenaar heus wel weet wat wel en niet mag, zonder dat er duidelijke regels zijn.

Is de civiele rechter bereid om met een schuin oog te kijken naar de jurisprudentie van de ambtenarenrechter in vergelijkbare zaken?

Er zijn uitspraken van civiele rechters die de wenkbrauwen van overheidswerkgevers doen fronsen. Aardig is bijvoorbeeld een uitspraak van het Gerechtshof Arnhem-Leeuwarden over een ruimhartig declarerende medewerker die op creatieve wijze invulling gaf aan de mogelijkheden tot het declareren van lunches en diners. Weliswaar gold er een uitvoerige regeling bij zijn werkgever (SKF) met als veelzeggende titel 'Declareren, dat doe je zo', doch het Hof vond deze niet duidelijk. Zo was er volgens het Hof niet duidelijk omschreven wat als lunch of avondmaaltijd moest worden beschouwd, zodat de invulling daarvan ter vrije bepaling van de werknemer stond:

"Indien SKF van mening zou zijn geweest dat bepaalde eet- en drinkwaren niet zouden mogen vallen onder de noemer lunch of avondmaaltijd, dan had zij hiervoor nadere regels moeten opstellen.", aldus het Hof.

Ondanks het feit dat de declaraties op zijn minst dubieus waren, dat betrokkene een aantal malen maaltijden had gedeclareerd die hij tezamen met zijn gezin had genuttigd en dat hij zichzelf in het kader van het onderzoek had tegengesproken, bleef het ontslag op staande voet niet in stand.

Daar staat tegenover een uitspraak van de Centrale Raad van Beroep over een strafontslag vanwege onder meer het declareren van 1,075 kg appels als lunch. Ook hier stelde de betrokkene dat niet helemaal duidelijk was wat gedeclareerd mocht worden. De Raad maakte daar korte metten mee. Volgens hem is een kilo appels evident géén lunch: "Voor zover appellant heeft gesteld dat hij er niet van op de hoogte was wat nu wel of niet mocht worden gedeclareerd, is de Raad van oordeel dat dit hem niet vrijpleit."

Groot gewicht hechtte de Raad aan de eigen verantwoordelijkheid van de medewerker. Ook de gebrekkige controle speelde geen rol van betekenis: "Dat bij eerdere controle de onjuistheid van declaraties wellicht voor een groot deel had kunnen worden onderkend, vormt onvoldoende grond voor een ander oordeel.", aldus de Raad.

Eén van de vragen die zich na 1 januari 2020 voordoen, is of de civiele rechter bereid is om met een schuin oog te kijken naar de strenge jurisprudentie van de ambtenarenrechter in vergelijkbare zaken. Voor overheidswerkgevers is vooral van belang dat zij vóór 1 januari 2020 nog eens goed moeten kijken naar hun bestaande integriteitsbeleid en de schriftelijke vastlegging daarvan. Zij moeten rekening houden met de strenge eisen die in de arbeidsrechtelijke jurisprudentie worden gesteld op dit punt.

Hoffmann

Vertrouwen is goed,

Hoffmann is beter

Hoffmann
Uw veiligheid, daar maken we ons sterk voor, al meer dan 55 jaar. Hoffmann bestaat uit drie afdelingen: bedrijfsrecherche, riskmanagement en cybersecurity.

Bedrijfsrecherche
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.

Riskmanagement
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 aan een veilige werkomgeving. Ze helpen u veilige processen en effectieve controles in te richten, maar vooral met het toewerken naar een veilige en integere cultuur. Met als uitgangspunt: veiligheid zie je niet, die voel je.

Cybersecurity
Uw bedrijfsinformatie is uw goud. Dat houdt u graag in veilige handen. In de digitale wereld waarin we leven is dat niet zo eenvoudig. Vaak zijn daar beter beveiligde netwerken, goed doordachte processen en cyberbewuste medewerkers voor nodig. Met preventief onderzoek naar uw informatiebeveiliging maken wij inzichtelijk wat uw kroonjuwelen zijn en waar voor u de risico's liggen.

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