8 tips om fraude in uw onderneming te voorkomen

WHISTLEBLOWER PARTNERS

Bedrijfsfraude is een groot en toenemend probleem nu de globalisering, digitalisering en de toegenomen complexiteit op vele gebieden, zoals bijvoorbeeld Covid-19, het risico hebben vergroot.

Fraude binnen bedrijven is een groter probleem dan veel mensen denken. Een onderneming kan tot vijf procent van haar jaaromzet verliezen door interne fraude. Dit blijkt uit internationale studies. Nederlandse bedrijven zien ook een sterke toename van financiële cybercriminaliteit, waarbij de medewerkers misleid worden om geld te betalen aan externe criminelen.

Het moge duidelijk zijn dat controle hierbij essentieel is. Auditing tools kunnen weliswaar behulpzaam zijn, maar de oplossing is helaas niet zo eenvoudig. Net zo belangrijk is een goede werkcultuur waarin medewerkers worden aangemoedigd en beïnvloed om de juiste keuzes te maken. Ze maken dan geen bewuste of onbewuste fouten die het bedrijf duur kunnen komen te staan.

Sinds de Covid-19 epidemie ons heeft getroffen, is thuiswerken het nieuwe normaal geworden en deze trend zal zich waarschijnlijk voortzetten. Dit heeft ook nieuwe risico's voor het bedrijfsleven met zich meegebracht.
Hier volgen enkele aandachtspunten met betrekking tot bedrijfsfraude:

1. **Verhoogde controle en aandacht voor procedures in de onderneming**

Minder mensen op kantoor kan betekenen dat de procedures intern worden versoepeld om de dagelijkse gang van zaken gemakkelijk te laten verlopen. Collega´s delen wachtwoorden met elkaar en het risico bestaat dat een en dezelfde persoon zowel facturen kan goedkeuren als crediteurengegevens kan wijzigen en betalingen kan goedkeuren.
Dit biedt goede mogelijkheden voor financiële fraude, waarbij de fraudeur zijn sporen kan uitwissen. Als dit gedurende een lange periode op kleine schaal gebeurt, kan de fraude vrij omvangrijk worden voordat deze, misschien, wordt ontdekt.
Ondernemingen zouden hun interne procedures dan ook niet moeten versoepelen, al werken werknemers steeds vaker individueel vanuit huis en 'reguleren' zij de controleactiviteiten voortdurend aan de hand van de risico's.

2. **Vergroot het bewustzijn over hacking, phishing en andere IT-fraude**

Criminelen proberen steeds vaker bedrijven via telefoongesprekken (vishing), sms-berichten (smishing) of e-mails (phishing) ertoe te verleiden om persoonlijke codes of informatie te verstrekken. De fraudeur doet zich vaak voor als iemand van bijvoorbeeld de bank of een zakenpartner van het bedrijf, de overheid, NemID of Nets.
De e-mailsystemen van sommige bedrijven worden rechtstreeks gehackt, andere cyberfraudeurs maken gebruik van phishing, waarbij een klik op een link of bestand in een nep-e-mail toegang kan geven tot de IT-systemen van het bedrijf.

Het is van groot belang de werknemers ervan te doordringen dat zij sceptisch moeten zijn ten opzichte van ongevraagde contacten of e-mails die er ongewoon of vreemd uitzien. Tevens moeten de werknemers ervan doordrongen zijn dat zij nooit persoonlijke informatie of codes mogen verstrekken. In geval van twijfel moeten individuele werknemers altijd contact opnemen met de IT-afdeling van hun bedrijf - beter één keer te veel dan één keer te weinig.

3. **CEO-fraude voorkomen**

Er is sprake van CEO-fraude wanneer een werknemer wordt misleid om een valse factuur te betalen of een ongeoorloofde overschrijving uit te voeren vanaf de bedrijfsrekening naar een rekening die eigendom is van de oplichter. De oplichter doet zich voor als een hooggeplaatst persoon in het bedrijf.
Het is belangrijk dat het bedrijf procedures heeft voor het betalen van rekeningen en het overmaken van geld en dat alle verzoeken die niet normaal zijn, altijd worden gevolgd door een controle, hoe dringend de overmaking volgens de e-mail ook is. Eén telefoontje naar de CEO brengt vaak de hele fraude aan het licht en behoedt het bedrijf voor enorme verliezen.

4. **Factuurfraude voorkomen**

Bij factuurfraude of bedrog doet de oplichter alsof hij een klant of leverancier van het bedrijf vertegenwoordigt en vraagt hij om betaling van facturen naar een nieuwe bankrekening - die aan de oplichter toebehoort.
Het is van belang ervoor te zorgen dat het betrokken personeel op de hoogte en zich bewust is van dit soort fraude en hoe deze kan worden voorkomen. Het is dus van essentieel belang om het personeel dat met de betaling van facturen is belast te instrueren dat ze altijd op onregelmatigheden moeten controleren, dat er vaste procedures moeten zijn voor de behandeling van manuele betalingen en dat de rechtmatigheid van de betalingsverzoeken moet worden geverifieerd.
Het is handig om daarbij gebruik te maken van een geautomatiseerd betalingssysteem om het aantal manuele betalingen tot een minimum te beperken.

5. **Let op fraude bij het wijzigen van bankgegevens**

Het is belangrijk dat men zich ervan bewust is dat dit soort fraude met wijziging van bankgegevens bestaat. Deze kennis moet worden gedeeld met die functies binnen het bedrijf die mogelijk het slachtoffer worden van dergelijke wijzigingen van bankgegevens.
Indien het bedrijf een e-mail ontvangt over een wijziging in de bankgegevens, moet altijd contact worden opgenomen met de leverancier om de juistheid van de wijziging te verifiëren met de gebruikelijke contactpersoon van het bedrijf.

6. **Vermijd btw-fraude**

Er bestaat een aanzienlijk risico dat bedrijven worden blootgesteld aan btw-fraude wanneer zij handel drijven in verband met btw-carrousels. Btw-carrousels worden gekenmerkt door de grensoverschrijdende handel in goederen of diensten. Doorgaans worden de goederen verhandeld via een stroman die geen btw aangeeft of afdraagt wanneer de goederen worden doorverkocht. De goederen worden vervolgens verhandeld via een of meer tussenpersonen alvorens opnieuw uit Nederland te worden verzonden om de carrousel voort te zetten.
Deze tussenpersonen kunnen echte Nederlandse bedrijven zijn. Dit betekent dat Nederlandse bedrijven gemakkelijk in de val kunnen lopen die tot financiële verliezen kan leiden, bijvoorbeeld in de vorm van gederfde btw-aftrek, incourante goederen, een slechte reputatie of oneerlijke concurrentie in de bedrijfstak. In sommige gevallen kan een hele markt worden ondermijnd voordat de fraude wordt ontdekt.
Als er ook maar de geringste twijfel bestaat over de leverancier of de goederen die het bedrijf wil kopen, dan moet u ver van de deal blijven. En het verdient aanbeveling om altijd na te gaan of de bedrijven waarmee de onderneming handel drijft, voor de btw geregistreerd zijn. Het bedrijf doet dit door het btw-nummer van de leverancier op te zoeken.
Op de website van de belastingdienst vindt u ook een aantal specifieke punten waarop u moet letten bij de inkoop en verkoop van goederen.

7. **Pas op voor printers**

Printers in bedrijven kunnen, als men niet oppast, een aanzienlijk veiligheidsrisico vormen voor een bedrijf.
Ontwikkelingen in de printertechnologie, waaronder het feit dat printers dezelfde hardwarecomponenten bevatten als een computer, zoals een harddrive, bedieningspaneel en toetsenbord, betekenen dat bedrijven hun printers net als PC's moeten beveiligen tegen cyberaanvallen. Dit wordt vaak over het hoofd gezien, ook al zijn Nederlandse bedrijven zich over het algemeen zeer bewust van de cyberdreiging.

8. **Neem contact op met de bank en meld fraude of poging tot fraude bij de politie**

Indien de fraude is gepleegd via de bank van het bedrijf, moet altijd contact worden opgenomen met de bank om het bedrag eventueel terug te kunnen vorderen. Neem ook altijd contact op met de politie in geval van fraude of een poging tot fraude, zelfs als u niet het slachtoffer van fraude bent geworden. Vergeet niet om alle documentatie te bewaren en op te nemen in de aangifte bij de politie.