

Technologie zet de deur wagenwijd open voor fraudeur

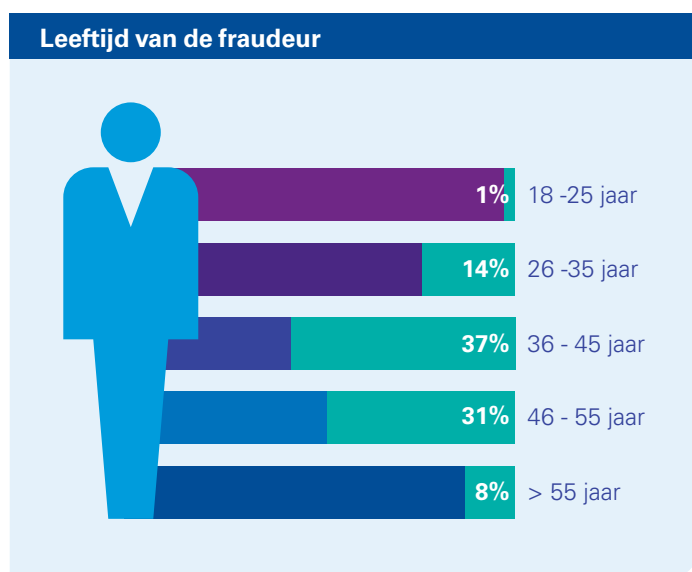


Het gebruik van technologie stelt ondernemingen in toenemende mate bloot aan fraude. Doordat interne controles vaak te wensen overlaten, kunnen fraudeurs ongehinderd hun gang gaan. Fraudepreventie blijft technologisch achter en vereist spreekwoordelijke gezien een meer 'oog om oog, tand om tand' benadering.

Het is een gegeven dat bedrijven wereldwijd schade ondervinden als gevolg van fraude. Naast de financiële en juridische implicaties wordt de maatschappelijke impact van fraude in tijden van transparantie steeds omvangrijker. KPMG onderzocht in totaal 750 fraudegevallen verdeeld over 78 landen over de periode 2013 tot 2015 om het profiel van de fraudeur in kaart te brengen en publiceerde in 2016 in de internationale publicatie "Global profiles of a fraudster". Uit dit onderzoek blijkt dat één op vier fraudes gepaard gaat met het gebruik van technologie.

Kenmerken fraudeur

"Global profiles of a fraudster" wijst uit dat de gemiddelde fraudeur internationaal gezien nog steeds man is, tussen de 36 en 55 jaar oud is, enige status binnen een bedrijf heeft en over de mogelijkheid beschikt om beheersingsmaatregelen ter zijde te schuiven. Daarnaast is er een grote kans dat de fraudeur op managementniveau of hoger opereert, minstens zes jaar werkzaam is in het bedrijf en door collega's als autocratisch wordt getypeerd. Internationaal gezien zijn de vrouwelijke fraudeurs bezig met een opmars. De Nederlandse fraudeur is in meer dan de helft van de gevallen onder de 45 jaar en daarmee een stuk jonger dan de internationale fraudeurs.



Bron: Global Profiles of the Fraudster, KPMG International, 2016

Fraudedreiging

De grootste fraudedreiging komt nog steeds van binnenuit, daar 65% van de fraudeurs een arbeidsrelatie heeft met de organisatie waarbinnen de fraude zich manifesteert. Bij een kwart van de fraudedelicten is gebruik gemaakt van technologie. Technologie is daarmee een belangrijk vliegwiel voor fraudeurs om de fraude daadwerkelijk te plegen. Dit soort delicten wordt gepleegd door jongeren (tussen de 26 en 45 jaar) die over een meer dan gemiddelde kennis van de technologie beschikken. Het feit dat dit soort fraudes vooral in deze leeftijdscategorie plaatsvindt betekent dat de omvang van de elektronische delicten alleen maar zal toenemen.

Bij 24% van alle technologiedelicten werd vervalste of misleidende informatie ingevoerd in de administratie, in 20% van de gevallen wist de fraudeur via email of een ander berichtenplatform informatie te vervalsen en bij 13% van de fraudes maakte de fraudeur misbruik van de toegang die hij had tot de computersystemen.

Cyberfraude

Hoeveel op dit moment de grootste fraudedreiging van binnenuit komt, voorziet KPMG dat in de loop der jaren de fraudedreiging buiten de organisatie verder zal toenemen. Op dit moment kan 4% van de geanalyseerde fraudes worden aangemerkt als cyberfraude. Op het eerste gezicht lijkt het aandeel van cyberfraude beperkt, maar dit zou het topje van de ijsberg kunnen zijn. Veel fraude via het internet blijft nog altijd onopgemerkt. Naast de externe frauderisico's als gevolg van cyberincidenten kan worden gedacht aan de risico's die ondernemingen lopen als gevolg van externe partijen die (internationaal) namens de onderneming opereren.

Daarnaast is de fraudeur vooral uit op het in het bezit krijgen van emails van het management en belangrijke strategische informatie van het bedrijf. Ook een DoS, een denial of services, waarbij gebruikers geen toegang krijgen tot een computersysteem, vormt vaak het doelwit. Uit de praktijk blijkt dat veel ondernemingen nog altijd onvoldoende in staat zijn om zich te wapenen tegen cyberfraude.

Tegenwicht

De inspanningen van fraudeurs om nieuwe technologie te gebruiken om de beheersingsmaatregelen te omzeilen loopt uit de pas met de inspanningen van bedrijven om fraude met behulp van technologie juist te voorkomen. In Nederland kwamen de meeste fraudes aan het licht door de fraudeur

zelf. In 20% van de fraudegevallen rees een verdenking doordat een fraudeur zelf per ongeluk informatie vrijgaf. Slechts 3% van de onderzochte fraudes is proactief opgespoord behulp van technologie, waaronder het inzetten van anti-fraude 'Data Analytics' of 'Open Source Intelligence' om delicten en risicovolle zakenpartners vroegtijdig op te sporen.

Het belang van het screenen van zakenpartners en andere partners, die namens een onderneming kunnen opereren, neemt aanzienlijk toe. Veel bedrijven opereren steeds internationaler en worden steeds afhankelijker van dit soort partijen die vaak optreden als distributeur, agent of lokaal vertegenwoordiger. Onderzoek naar de risico's van externe partijen zou onderdeel moeten uitmaken van het compliance programma van bedrijven.

Breng daarom periodiek de interne en externe frauderisico's in kaart en zet daar adequate (technologische) beheersingsmaatregelen tegenover naast aandacht voor de organisatiecultuur. Het profiel van de fraudeur is immers aan het veranderen en daarmee de verschijningsvormen van fraude. Het bewust nadenken over interne en externe frauderisico's en het proactief inzetten van technologie vergroot de weerbaarheid van een organisatie.

Voorkomen is immers altijd beter dan genezen.

Het gebruik van technologie bij het plegen van de fraude



Bron: Global Profiles of the Fraudster, KPMG International, 2016

Contact:

Jack de Raad

Partner

T: +31(0)20 656 7774

E: deraad.jack@kpmg.nl

Caroline Molenaar

Director

T: +31(0)70 338 2138

E: molenaar.caroline@kpmg.nl

De in dit document vervatte informatie is van algemene aard en is niet toegespitst op de specifieke omstandigheden van een bepaalde persoon of entiteit. Wij streven ernaar juiste en tijdige informatie te verstrekken. Wij kunnen echter geen garantie geven dat dergelijke informatie op de datum waarop zij wordt ontvangen nog juist is of in de toekomst blijft. Daarom adviseren wij u op grond van deze informatie geen beslissingen te nemen behoudens op grond van advies van deskundigen na een grondig onderzoek van de desbetreffende situatie.

© 2016 KPMG Advisory N.V., ingeschreven bij het handelsregister in Nederland onder nummer 33263682, is lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Cooperative ('KPMG International'), een Zwitserse entiteit. Alle rechten voorbehouden.