HOUTHOFF

Factsheet CEO-fraude

Een onderneming kan slachtoffer worden van en benadeeld worden door strafbare feiten. Zie voor algemene informatie hierover de Factsheet benadeling door strafbare feiten. Als een onderneming slachtoffer wordt van fraude, gebeurt dat steeds vaker door gebruik te maken van computers en het internet en wordt gesproken van cybercrime. Een vorm van cybercrime die steeds vaker voorkomt is de CEO-fraude, ook wel bekend als whaling. Bij een CEO-fraude doen fraudeurs zich voor als CEO of andere leidinggevende, meestal met als doel dat een collega van de zogenaamde directeur onterecht betalingen verricht of laat verrichten aan de fraudeurs.

Patronen CEO-fraude

Een CEO-fraude kan veel verschijningsvormen hebben. Vaak zoekt de zogenaamde CEO contact met een medewerker in verband met een urgent en vertrouwelijk project, zoals de overname van een ander bedrijf. De daders benadrukken dat het project niet met andere collega's gedeeld mag worden, al dan niet omdat sprake is van beursgevoelige informatie en/of omdat de vermeende overname nog moet worden goedgekeurd door een overheidsinstantie. Hierbij worden ook geheimhoudingsverklaringen (NDA's) gebruikt en andere formele documenten die indruk maken op het slachtoffer. Bij internationale ondernemingen doen de daders zich meestal voor als CEO van de buitenlandse moederorganisatie. Bij CEO-fraude worden steeds geavanceerdere technieken gebruikt, zoals deepfake technologie. Met die technologie kan de CEO overtuigend worden geïmiteerd, met zowel audio als videobeelden.

In het kader van het zogenaamde project wordt op enig moment verzocht betalingen te doen, meestal in tranches en naar verschillende buitenlandse bankrekeningen. Vaak weten de daders al dat het slachtoffer intern de bevoegdheid heeft om de betreffende betalingen te laten uitvoeren. De daders spelen in op het slachtoffer door te bedanken voor de medewerking en te suggereren dat het slachtoffer beloond zal worden voor diens hulp.

Signalen van CEO-fraude

Enkele voorbeelden van signalen van CEO-fraude zijn:

- De daders maken gebruik van e-mail-adressen waarvan de extensie niet overeenkomt met de authentieke extensie van de organisatie.
- Voor de communicatie gebruiken de daders communicatievormen die niet gebruikelijk zijn binnen de organisatie, zoals een afwijkende applicatie voor videocalls of het gebruik van audioberichten via WhatsApp.
- Als het slachtoffer voorstelt de kwestie te bespreken met collega's of met de CEO zelf via andere kanalen dan gehanteerd door de daders, reageren de daders afwijzend. Zij bedenken redenen dat het slachtoffer de kwestie zelfs niet met de CEO zelf mag bespreken. Bij enige twijfel of sprake is van CEO-fraude is het daarom belangrijk om persoonlijk contact met de CEO te zoeken, via de officiële contactgegevens in plaats van de gegevens die de daders gebruiken. Een verificatie per e-mail geeft geen volledig uitsluitsel omdat het mogelijk is dat het e-mailaccount van de CEO is gehackt.
- De daders vermijden telefonisch contact als het slachtoffer hen zelf benadert. Als het slachtoffer zelf probeert contact te zoeken, zijn de daders niet bereikbaar en/of vragen zij om een e-mail of Whatsapp-bericht te sturen omdat de zogenaamde CEO het te druk heeft. Dit omdat de deepfake technologie niet of minder goed werkt wanneer de daders spontaan een imitatie moeten uitvoeren.
- Hoewel de kwaliteit van deepfakes steeds beter wordt, is de geluid- en beeldkwaliteit van het door de daders

gebruikte communicatiemiddel soms slecht en zit er vertraging tussen video en audio. Gezichtsuitdrukkingen kunnen er ook onrealistisch uitzien.

- De bedrijven waaraan de betalingen moeten worden verricht zijn buitenlandse partijen die onbekend zijn die bij nader inzien ook niet passen bij het verhaal van de fraudeurs. Vaak betreft het recent opgerichte bedrijven die geen aantoonbare bedrijfsactiviteiten verrichten. Dit betreft vaak bedrijven uit Oost-Europa of Azië.
- Collega's of de bank van de onderneming stellen kritische vragen over de achtergrond van de (voorgenomen) betalingen. Het is altijd belangrijk om dit soort signalen serieus te nemen en onafhankelijk te beoordelen. Als deze signalen worden gedeeld met de daders, komen zij vaak met een weerlegging en/of stellen zij voor hoe de partij die de vragen heeft gesteld gerust moet worden gesteld.

Aangifte doen en andere vervolgstappen

Bij CEO-fraude wordt vaak gebruikgemaakt van een web aan buitenlandse bedrijven en bankrekeningen. Geld dat eenmaal is overgemaakt wordt vaak direct doorbetaald aan andere buitenlandse rekeningen. Hierdoor is het lastig de daders op te sporen en het geld terug te krijgen. Toch kan het mogelijk zijn om het geld (deels) terug te halen, mits er tijdig en adequaat wordt gehandeld. Bij signalen van CEO-fraude is het met name belangrijk om een eventuele aangifte zo snel mogelijk bij de juiste plek te doen. In samenwerking met de autoriteiten en eventueel een forensisch accountant kan worden beoordeeld welk onderzoek mogelijk is en of ook autoriteiten en advocatenkantoren in het buitenland worden betrokken. Daarnaast kan worden beoordeeld of er naast een aangifte mogelijkheden zijn voor civielrechtelijke stappen, zoals het leggen van beslag op banksaldi die nog beschikbaar zijn. Deze stappen vergen snelheid en een goede kosten-baten analyse van de stappen die naar verwachting het meeste rendement hebben.

Contact

Als u vragen heeft over deze factsheet kunt u mailen naar of contact opnemen met onderstaande personen.

Frank Mattheijer
Advocaat | Counsel

T +31 20 605 69 12
M +31 6 4239 2742
f.mattheijer@houthoff.com

Marianne Bloos
Advocaat | Of Counsel

T +31 20 605 62 05
M +31 6 5324 0328
m.bloos@houthoff.com