INTERVIEW

SECUREME2

neotopia

CEO-fraude: ons gedrag is de zwakste schakel

“Het idee dat met name oudere consumenten slachtoffer zijn is inmiddels achterhaald.”

CEO-fraude: ons gedrag is de zwakste schakel

Het is 24 februari 2022. RTL nieuws *kopt “Rotterdams staalbedrijf slachtoffer ceo-fraude, buit 11 miljoen.”* Het is slechts één van de vele voorbeelden van CEO-fraude van de afgelopen jaren. De schade loopt in de vele miljoenen. Het idee dat met name oudere consumenten slachtoffer zijn - van neptelefoontjes van zogenaamde bank-medewerkers met niet al te beste intenties - is inmiddels achterhaald. Het bedrijfsleven krijgt ongewenst veel aandacht van (internet)criminelen. Veelal met enorme financiële gevolgen van dien.

Een interview over ceo-fraude met Daniël Prins (SecureMe2) en Joost Kerkhofs (Neotopia). Wat is het? En wat kan Organizational Behavior Management (OBM) betekenen in de strijd tegen ceo-fraude?

Daniël, jij maakt je zorgen?

D: “Dat zou je zo kunnen stellen. Wat ik in mijn werk steeds vaker zie is dat de creativiteit van de boze buitenwereld, zeg maar gerust criminelen, toeneemt. De financiële omvang van fraudegevallen is momenteel echt gigantisch.

Ik maak me daar zorgen over en wil mensen behoeden voor het maken van onnodige fouten. Natuurlijk, de criminelen zijn de daders, maar WIJ kunnen ons gedrag aanpassen en ons behoeden van de catastrofale gevolgen die ceo-fraude met zich meebrengt."

Lijkt me interessant om straks wat verder door te praten over het gedragscomponent. Maar eerst ceo-fraude. Wat is dat eigenlijk?

D: "In het er kort komt het erop neer dat een ogenschijnlijk interne mail wordt verstuurd met het verzoek geld over te maken. Bijvoorbeeld vanwege een investering die het hoofdkantoor wil doen. Het dossier lijkt correct. Echter, het daarop vermelde buitenlandse bankrekeningnummer wijkt af van het rekeningnummer dat we gewend zijn. In werkelijkheid is de zogenaamde interne mail helemaal geen bericht van een collega, maar komt deze van een andere mailserver en het rekeningnummer is van een andere begunstigde."

Ok, en dan?

D: "In het bericht wordt de noodzaak aangegeven. Het geld moet zo spoedig mogelijk overgemaakt worden. Het bericht lijkt te zijn verstuurd door iemand met status, bijvoorbeeld de CEO. Kortom, wie het bericht ontvangt wordt dan toch wat onrustig. Wat je vervolgens vaak ziet is dat men niet handelt volgens de interne procedures, als die er al zijn. Het geldt wordt overgemaakt op de rekening en dan is één ding zeker: het geld is weg!"

"Ik maak me zorgen en wil mensen behoeden voor het maken van onnodige fouten. Natuurlijk, de criminelen zijn de daders, maar WIJ kunnen ons gedrag aanpassen."

Daniël Prins (SecureMe2)

Maar dat zijn toch vaak criminelen uit het buitenland die de Nederlandse taal niet goed machtig zijn? Daar trap je toch niet zomaar in?

D: “De criminelen worden steeds handiger. Laatst kwam ik een geval tegen bij een opdrachtgever waarbij er niet alleen een ‘intern’ betaalverzoek was verstuurd, maar deze was ook nog eens voorzien van een onderzoek van een ‘gerenommeerd advocatenkantoor’. Vervolgens nam de zogenaamde advocaat ook nog eens contact op om het nep-dossier toe te lichten. Kortom, vaarwel amateuristische phishing mails met spel- en typefouten en inhoudelijk onzin! Je ziet nu vooral nog een professioneel opgebouwd intern dossier dat ook nog eens inspeelt op het gemak van de ontvanger.”

“Vaarwel amateuristische phishing mails met spel- en typefouten en inhoudelijk onzin!”

Joost, jij bent expert op het gebied van gedrag. Wat maakt dat de ontvanger niet op onderzoek uitgaat en gewoon even de telefoon pakt om te checken of hij met de echte verzender belt?

J: “Het begint bij het besef dat je kennis over gedrag nodig hebt om het te kunnen veranderen. Kennis zorgt ervoor dat we mensen optimaal kunnen beïnvloeden om het gewenste gedrag te vertonen. Het lijkt erop dat de internetcriminelen die kennis al hebben én het keihard tegen ons gebruikt om gedrag te beïnvloeden. Het is tijd om zelf ook beter te snappen wat gedrag precies is en hoe het werkt, zodat we ons beter kunnen wapenen tegen dit soort malversaties.”

Oké, kennis is dus nodig. Laten we dan beginnen bij: wat *is* gedrag eigenlijk?

J: "Prima startpunt, haha! In het kort: alle waarneembare, actieve handelingen van een levend wezen. Denk voorbeeld aan het aanzetten van je computer of het openen van je mailbox. En dus ook 'klikken op een link in een phishing-mailtje'. Vraag je daarbij af: kan ik het gedrag filmen en levert dat een actiefilm op? Zo ja, dan is het gedrag."

Je had het eerder over gewenst gedrag. Wat is dat dan en hoe stuur je daarop?

J: "Tja, dat valt te bezien. Als we kijken naar 'klikken op een link in een phishing-mailtje' dan is dat vanuit twee partijen bezien gedrag, maar voor de criminelen is het wenselijk en voor het slachtoffer onwenselijk gedrag. Vervolgens kijk ik vooral naar de gevolgen voor de persoon die het gedrag vertoont. Dus niet voor een ander, of de organisatie als geheel, maar voor de presteerder van het gedrag persoonlijk."

Dan heb je het dus over het werkelijke beïnvloedingsproces in ons brein?

J: "Inderdaad. En dan helpt het om heel specifiek en concreet te zijn. Ons brein is namelijk zo opgebouwd dat het die informatie nodig heeft om te *leren.* En leren doen we door ervaringen op te bouwen over wat wel en niet werkt. In die zin een mooie vergelijking met programmeren: 'als dit, dan dat'. Ons brein is een leermachine die constant aan staat. Verreweg het meeste gedrag dat we vertonen is aangeleerd. En we weten inmiddels dat bij positieve consequenties van gedrag dopamine vrijkomt. Dopamine is een verslavend stofje dat je een goed gevoel geeft. Kortom, je wilt als presteerder maar al te graag het gedrag herhalen."

Dus als je dit weet, heb je in feite de macht?

J: "Klopt! En niet alleen de fraudeur waar we het eerder over hadden weet dit. Ook de gok-industrie, social media platformen, de gaming sector en marketeers van loyaliteitsprogramma's gebruiken deze kennis al heel lang om ons gedrag te vormen. Ze laten ons positieve ervaringen beleven waardoor die dopamine gaat vloeien in ons brein."

Ok, dat is helder verwoord! Nu dan die casus over ceo-fraude. Hoe verklaar je dan dat we 'erin trappen'?

J: "Een verzoek van een CEO om iets te doen, en wel snel, met een eenvoudige handeling, is erg verleidelijk: we kunnen met één muisklik iemand uit de brand helpen! En meteen daarna ook weer door met andere zaken! Hoe fijn is dat!? En dan kun je ook nog eens iemand uit de top helpen. Dat is vast heel goed voor je carrière, toch? Maar misschien juist ook niet zo goed voor je carrière wanneer je het NIET doet. Beide factoren spelen mee.

Joost Kerkhofs (Neotopia)

Hoe krijgen we hier meer kennis over?

J: “Om organisaties hier vertrouwd mee te laten raken en te helpen de juiste interventies te doen is er vanuit de wetenschap inmiddels een gevalideerde en bewezen aanpak, die leidt tot meetbare prestatieverbeteringen.

Organizational Behavior Management (OBM) wordt wereldwijd toegepast op prestatie-vraagstukken op het gebied van productiviteit, kwaliteit en veiligheid. Cybersecurity zou daar zomaar eens met recht als aandachtsgebied aan toegevoegd kunnen worden.”

Niet zo gek Daniël, dat je met veel kansen ziet voor OBM binnen cybersecurity!

D: “Dat klopt zeker! In de dagelijks praktijk werk ik vanuit mijn rol bij SecureMe2 voor verschillende organisaties om deze door inzet van een actieve netwerkmonitoringsoplossing weerbaar te maken voor netwerk- en internetfraude. We zijn als het ware een tech-nisch vangnet, omdat we weten dat we het gedrag nooit voor de volle 100% kunnen beïnvloeden. Het positieve vind ik nu wel: met OBM is er als het ware een nieuw en bewezen vangnet voor gedrag gecreëerd. Eén die de kans op positieve aanpassingen in het gedrag aan-zienlijk vergroot. De nieuwste technieken en gedragsinterventies gaan wat mij betreft dan ook hand in hand. Ze kunnen niet zonder elkaar.”

Meer weten?

Neotopia.nl

Joost Kerkhofs
06-20890344
J.kerkhofs@neotopia.nl

Mattenbieslaan 103
3452 AD Vleuten

KvK: 34300818

OBM - CYBER SECURITY - INTERVIEW