Resultaten van een awareness-training in het herkennen van phishingmails

Dieke Miltenburg*

Een probleem bij digitale criminaliteit is dat slachtoffers vaak niet weten dat ze slachtoffer zijn en ook als ze dat wel weten, geen aangifte doen bij de politie. Derhalve is weinig informatie beschikbaar over de kenmerken van slachtoffers van digitale criminaliteit. Verscheidene onderzoekers hebben getracht hier meer inzicht in te verkrijgen door aan respondenten scenario's voor te leggen. Hierbij is respondenten gevraagd om phishingmails van legitieme mails te onderscheiden, zowel voorafgaand aan als na afloop van een training over dit onderwerp. Probleem bij dit soort onderzoek is dat de respondenten weten dat ze aan een test meewerken. Het is dan ook goed mogelijk dat zij in het dagelijks leven andere keuzes zouden maken dan in het testscenario.

Derhalve is voor een andere aanpak gekozen bij een onderzoek naar het klikgedrag van ondernemers bij het ontvangen van phishingmails voor en na een *awareness*-training. De deelnemers konden zich inschrijven voor een 'weerbaarheidstest', waarbij niet werd verteld dat het een phishingtest betrof. De deelnemers aan de test ontvingen, verspreid over drie rondes, in totaal zes phishingmails. Na het versturen is bijgehouden of, en zo ja, wie van de ondernemers op een link in een of beide mails hadden geklikt en of zij gegevens achterlieten op de websites waar de link in de mail naartoe verwees. De eerste ronde van twee phishingmails vond plaats in de week voorafgaand aan de training (Ronde 1). Na Ronde 1 volgde een *awareness*-training, waarbij is stilgestaan bij het voorkomen van slachtofferschap van cybercrime in het algemeen en phishing in het bijzonder. De trainer gaf tips en liet zien waar ondernemers op dienen te letten bij het ontvangen van (phishing)mails, en hij beantwoordde tevens vragen vanuit de zaal. Een week na de training vond Ronde 2 plaats, waarin wederom twee phish-

* D. Miltenburg MSc behaalde recent haar wo-master Opsporingscriminologie aan de Vrije Universiteit Amsterdam. Deze bijdrage is gebaseerd op haar afstudeerscriptie, zie www.ubvu.vu.nl/pub/fulltext/scripties/14_2650385_0.pdf.

doi: 10.5553/JV/016758502020046002008

ingmails zijn verstuurd. Tot slot vond een maand na het volgen van de training Ronde 3 plaats, waarin de laatste twee phishingmails zijn verstuurd naar de deelnemende ondernemers.

Toen het klikgedrag van Ronde 1 vergeleken werd met Ronde 2, bleken in Ronde 2 significant minder ondernemers te hebben geklikt op een phishinglink dan in Ronde 1 (van 40,2% naar 25,0%). Eenzelfde significant verschil was zichtbaar bij de vergelijking tussen Ronde 1 en Ronde 3 (van 40,2% naar 26,0%). Tussen Ronde 2 en Ronde 3 was geen significant verschil aanwezig. Het aantal keer dat gegevens zijn achtergelaten op een phishingmail is afgenomen van 34 (Ronde 1) naar 14 (Ronde 2) en 16 (Ronde 3) keer. Uit het onderzoek is verder een significant verschil gebleken tussen mannen en vrouwen, waarbij, in tegenstelling tot eerder onderzoek, onder de groep mannen een hoger percentage op een link klikte dan onder de groep vrouwen. Man zijn bleek tevens een significante voorspeller voor het klikken op een link in ten minste een van de zes phishingmails. Het ontbreken van significante verschillen in leeftijd, opleidingsniveau, sector waarin iemand werkzaam is, en of iemand een eerdere *awareness*-training heeft gevolgd op het gebied van cybercrime, komt mogelijk door het beperkte aantal respondenten (n=92).

Naast het beperkte aantal respondenten ontbrak een controlegroep en is gebruik gemaakt van zelfbedachte bedrijven en scenario's, waarbij respondenten de phishingmails mogelijk voor spam hebben aangezien en niet voor phishing. Dit blijft gissen omdat met de respondenten geen terugkoppeling is geweest omtrent beweegredenen voor het wel of niet klikken. Een aanbeveling voor toekomstig onderzoek is dan ook om het kwantitatieve deel van het klikgedrag te combineren met een kwalitatief deel. Door respondenten achteraf te bevragen over de keuzes die zij hebben gemaakt bij het ontvangen van een (phishing)mail, waar zij op hebben gelet en wat bij hen de doorslag heeft gegeven voor het wel of niet klikken, wordt inzicht verkregen in het beoordelingsproces. Daarnaast kan meer informatie worden verkregen over waarom de ene groep klikt en de andere niet, zodat duidelijk wordt welke groepen extra bescherming nodig hebben om slachtofferschap te voorkomen. Om dit te bewerkstelligen wordt aanbevolen om gebruik te blijven maken van een phishingtest in combinatie met een fysieke training, zodat gewerkt wordt met echte mensen, echte situaties en echte trainingen.

doi: 10.5553/JV/016758502020046002008