Helpdeskfraude in Nederland

Jildau Borwell*

Helpdeskfraude (*tech support scam*) is een cybercrimevorm die in 2011 in Nederland opkwam. Vanwege de impact en het grote aantal slachtoffers is in 2018 gestart met een integrale aanpak om helpdeskfraude te bestrijden. Bij helpdeskfraude heeft een slachtoffer telefonisch contact met een oplichter die zich voordoet als medewerker van een software- of socialmediabedrijf. Dit contact komt op drie mogelijke manieren tot stand:

a. Het slachtoffer wordt gebeld over zogenaamde problemen (virussen of verlopen licenties) met diens computer.
b. Er verschijnt een schermvullende pop-up met een virusmelding op de pc van het slachtoffer met het verzoek een telefoonnummer te bellen.
c. Het slachtoffer zoekt een helpdesk van een software- of socialmediabedrijf en vindt een telefoonnummer op een nep-helpdeskwebsite van de oplichters, of dit telefoonnummer wordt per ongeluk doorgegeven door een legitiem bedrijf.

Daders van helpdeskfraude gebruiken 'social engineering', waarmee ze door misleiding toegang krijgen tot de systemen en vertrouwelijke gegevens van slachtoffers. De oplichters overtuigen slachtoffers ervan om via een *Remote Access Tool*[1] de besturing van de pc over te nemen (zodat computervredebreuk plaatsvindt), zogenaamd om de problemen op te lossen. Vervolgens wordt vaak toegang verkregen tot de online bankomgeving van het slachtoffer en wordt veel geld afgeschreven.

De oudere leeftijdsgroepen zijn onder slachtoffers van helpdeskfraude oververtegenwoordigd. Van de aangevers en melders tussen 2016 en 2019 is bijna de helft (46%) tussen de 60 en 79 jaar (N=4.184). Het aantal aangiftes

* J. Borwell MSc werkt binnen de politie als senior cybercrimeanalist bij het cybercrimeteam van de Eenheid Noord-Nederland. Vanuit een landelijke themaverdeling heeft zij zich gespecialiseerd in helpdeskfraude, waarbij zij onder andere de rapportages schreef waarop deze kadertekst gebaseerd is. Daarnaast doet zij vanuit het lectoraat Cybersafety van de NHL Stenden Hogeschool in Leeuwarden promotieonderzoek naar de impact van cybercrime op slachtoffers.

1 Het gaat hier meestal om legitieme software, die bijvoorbeeld vaak door ICT-afdelingen wordt gebruikt om de besturing van computers van medewerkers binnen het bedrijf over te nemen voor ondersteuning.

doi: 10.5553/JV/016758502020046002005

en meldingen van helpdeskfraude piekte in 2017, nam in 2018 af en in 2019 weer toe. In deze periode is echter een daling in gemelde schadebedragen te zien, met een totaal van tegen de € 5 miljoen in 2017, tegen de € 3 miljoen in 2018 en € 2,6 miljoen in 2019. De schade van slachtoffers wordt meestal niet vergoed. Naast financiële impact rapporteren slachtoffers bovendien psychologische, sociale en lichamelijke impact, zoals stress, slaapproblemen en verlies van vertrouwen in andere mensen.

Vanwege het grote aantal slachtoffers en de impact van helpdeskfraude geven politie, Openbaar Ministerie en partners prioriteit aan de bestrijding ervan. In maart 2018 tekenden vertegenwoordigers van publieke partijen en private partijen uit de telecom-, software- en financiële sector daartoe een intentieverklaring, waarmee het startsein werd gegeven voor de Brede Coalitie ter verstoring van Tech Support Scams in Nederland. Doordat de opsporing bij helpdeskfraude moeizaam is (daders bevinden zich veelal in India en gebruiken anonimiseringstactieken in hun communicatie en financiële infrastructuur), ligt de nadruk op preventieve en verstorende maatregelen. Deze maatregelen worden genomen op basis van een gezamenlijke intelligencepositie, waarmee een barrièremodel is opgesteld om het criminele bedrijfsproces te verstoren. De aanpak bestaat bijvoorbeeld uit mediacampagnes, blokkeren van gebruikte telefoonnummers, offline halen van websites, blokkeren van transacties en aanpassen van misbruikte functionaliteiten van RAT's.

Toen de coalitie startte, kwam de variant waarbij slachtoffers door de oplichters gebeld werden verreweg het meest voor. Sindsdien is de prevalentie hiervan sterk gedaald. In 2019 vond een verschuiving plaats naar de variant waarbij slachtoffers zelf een telefoonnummer van een helpdesk zochten en bij de oplichters uitkwamen. Hoewel onzeker is of de verschuiving het gevolg is van de maatregelen, illustreert deze dat politie en haar partners alert moeten blijven op daders en hun modus operandi. Criminele bedrijfsprocessen moeten blijvend worden gemonitord om tot een succesvolle aanpak te komen. Dat geldt temeer bij cybercrime, waarbij criminelen hun werkwijzen snel ontwikkelen, aanpassen en onderling delen.

doi: 10.5553/JV/016758502020046002005