Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

29 911 Bestrijding georganiseerde criminaliteit

Nr. 273 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 20 februari 2020

Bij brief van 27 november 2019 heeft u mij gevraagd te reageren op de berichtgeving over de grote toename van bancaire fraude door middel van phishing, zoals bijvoorbeeld op de site van het RTL-nieuws van 26 november 2019[1]. Met deze brief voldoe ik aan dat verzoek.
In deze brief geef ik – na een korte beschouwing van dit fenomeen – aan welke maatregelen door alle betrokken publieke en private partijen zijn genomen.
Ik zend u deze brief mede namens de Staatssecretaris van Economische Zaken en Klimaat.

Ontwikkelingen rond bancaire fraude d.m.v. phishing

De Nederlandse Vereniging van Banken (NvB) heeft op 26 november jl. bericht[2] dat in de eerste helft van 2019 de schade door fraude in het betaalverkeer als gevolg van phishing en bankpasfraude met ongeveer een derde is toegenomen. Daarbij gaven de banken aan bijna twee maal zoveel meldingen van klanten te ontvangen over phishing via mobiele berichtendiensten zoal SMS en WhatsApp.
Zoals ik in mijn brief van 20 april 2018 over de aanpak van cybercrime[3] heb aangegeven hebben de toenemende digitalisering, de enorme schaalvoordelen daarvan en de mogelijkheid om overal ter wereld eenvoudig en snel contacten te leggen ook een keerzijde. Ook criminelen kunnen op grote schaal hun activiteiten via internet ontplooien. Zij doen dit ook steeds geraffineerder en door het goed inspelen op nieuwe ontwikkelingen, zoals het gebruik van betaalverzoeken.

[1] https://www.rtlnieuws.nl/tech/artikel/4934691/whatsapp-phishing-linkje-marktplaats-speurders-sms-bankpas-betalen.
[2] https://www.nvb.nl/nieuws/phishing-verschuift-naar-sms-en-whatsapp.
[3] Kamerstuk 28 684, nr. 522.

kst-29911-273
ISSN 0921 - 7371
's-Gravenhage 2020

Verschijningsvormen van bancaire fraude d.m.v. phishing

Phishing naar bancaire gegevens is een dynamisch en soms internationaal fenomeen met verschillende verschijnings- en organisatievormen. Het kan op kleine schaal gebeuren, bijvoorbeeld via de zogenaamde «1-cent-methode», waarbij een slachtoffer via een link naar een valse bankensite wordt geleid en zo zijn inloggegevens aan de fraudeur prijsgeeft. Maar het kan ook op grote schaal gebeuren, waarbij (hele) grote groepen slachtoffers tegelijkertijd benaderd worden. Op het misbruik van telecommunicatievoorzieningen bij phishing wordt hieronder nader ingegaan.
Het criminele proces rond dit soort phishing kenmerkt zich door vele procesmatige stappen benodigd om het delict te kunnen plegen en door de gelaagdheid en de bedrijfsmatige insteek daarvan. Meerdere individuen plegen in vereniging, soms zonder van elkaars bestaan te weten, in verschillende fasen het delict in totaliteit, van verantwoordelijke kopstukken tot katvangers en moneymules[4].

Reactie

De aanpak van digitale betaalfraude, waaronder phishing, wordt door het kabinet zeer serieus genomen. Het kabinet heeft op 11 december 2019 een wetsvoorstel in consultatie gebracht ter implementatie van een Europese richtlijn[5] waarin fraude met digitale betaalmethoden apart strafbaar wordt gesteld en waar hogere straffen op komen te staan. Voor digitale betaalfraude kunnen op grond van dit wetsvoorstel gevangenisstraffen worden opgelegd tot zes jaar. De Europese richtlijn zorgt ervoor dat verschillende vormen van digitale betaalfraude, waaronder phishing en bijvoorbeeld ook de handel in gestolen betaalgegevens, in alle EU-lidstaten strafbaar wordt gesteld en draagt eraan bij dat lidstaten beter kunnen samenwerken bij de aanpak van deze grensoverschrijdende vorm van criminaliteit.

Preventie

Zoals ik meermaals met uw Kamer heb besproken is uiteindelijk de meest effectieve manier om fraude, waaronder bancaire fraude door middel van phishing te bestrijden, het voorkómen daarvan. Dit begint met de alertheid van de mensen zelf, bijvoorbeeld bij het klikken op links. Om die alertheid te vergroten heb ik in 2019 samen met een groot aantal publieke en private partijen, waaronder de banken, de publiekscampagne «Eerst checken, dan klikken» uitgevoerd[6].

Ook private partijen, zoals banken en online handelsplaatsen, spannen zich in om fraude, waaronder phishing, te voorkomen en te bestrijden. Zoals ik ook in mijn brief van 5 april 2019[7] aan uw Kamer heb bericht investeren banken continue in hun fraudemonitoring en -detectiesystemen en in voorlichting. Daarbij werken banken intensief met elkaar en andere betrokken private en publieke partijen samen, onder andere ten behoeve van de opsporing. Zo delen zij o.a. kennis over bijvoorbeeld de modus operandi bij phishing in het bancaire domein, zodat detectiesystemen steeds verrijkt kunnen worden met nieuwe regels

---

[4] Zie bijvoorbeeld: https://www.ad.nl/tech/man-verliest-een-miljoen-euro-met-bankpasfraude-hij-stuurde-z-n-pasje-op~ae777509/.
[5] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/12/11/mvt-wetsvoorstel-implementatie-van-de-richtlijn-2019-713-eu-van-het-europees-parlement-en-de-raad-over-bestrijding-van-fraude-met-en-vervalsing-van-niet-contante-betaalmiddelen.
[6] https://veiliginternetten.nl/maakhetzeniettemakkelijk/.
[7] Kamerstuk 29 911, nr. 237.

om die phishing te voorkomen. Met de politie wordt hiertoe o.a. samengewerkt binnen de Electronic Crime Task Force (ECTF). In de afgelopen jaren is phishing naar bancaire gegevens prominent aan de orde gekomen in diverse voorlichtingsactiviteiten van de banken, bijvoorbeeld via gemeenschappelijke campagnes zoals «Hang op, klik weg, bel uw bank» websites zoals https://www.veiligbankieren.nl/, en via websites van individuele banken.
De bank vergoedt schade van het slachtoffer van bancaire fraude door phishing, tenzij dat slachtoffer zelf frauduleus of grof nalatig heeft gehandeld. Basis hiervoor zijn de Uniforme Veiligheidsregels[8]. In het eerste half jaar van 2019 werd 97,9% van de schade door dergelijke phishing aan de klant vergoed.
Zoals ik tijdens het AO Criminaliteitsbestrijding op 5 februari jl. aangaf spreek ik halverwege maart opnieuw met de voorzitter van de Nederlandse Vereniging van Banken over de aanpak van fraude en in het bijzonder over de aanpak van katvangers én over de voortgang van de gesprekken tussen politie en banken over de intensivering van de samenwerking ten behoeve van fraudepreventie en zorg voor slachtoffers binnen het Landelijk Meldpunt Internetoplichting (LMIO).

Ook de online handelsplaatsen geven aan dat de belangrijkste manier om phishing naar bancaire gegevens te voorkomen het voorlichten van gebruikers is over veilig handelen en het herkennen van phishing(pogingen). Marktplaats heeft aangegeven hiertoe samen te werken met politie en andere partijen zoals banken en payment service providers. Daarbij worden ook modus operandi uitgewisseld. Marktplaats is doorlopend bezig met het ontwikkelen en toepassen van (al dan niet technische) maatregelen om phishing te bestrijden. Zo worden onder andere gebruikers gewaarschuwd op te letten zodra een link in een chatgesprek wordt ingevoerd, worden frauduleuze links in chatgesprekken geblokkeerd en biedt Marktplaats bescherming tegen phishing middels onder andere 2-factor authenticatie en een veilige betaaloplossing.
Ook organisaties zoals de Fraudehelpdesk waarschuwen actief.

Inzet OM en politie (oa binnen het ECTF)

De politie werkt nauw samen met de banken bij de bestrijding van phishing in het bancaire domein, o.a. binnen de hiervoor genoemde ECTF bij het Team High Tech Crime. Naast opsporing zetten politie en ECTF in op verstoring en preventie. Gelet op de aanhoudende phishingaanvallen tegen klanten van banken en de daarmee gepaard gaande schadelast is de ECTF in januari 2019 het project NoMorePhishing gestart, een breed offensief van publieke en private partijen ter bestrijding van phishing met als doel het aantal slachtoffers en de schadelast voor onder andere de bankensector drastisch te reduceren. Dit project heeft zich in het afgelopen jaar gericht op phishing van (bancaire) inloggegevens binnen de Nederlandse markt. Daarbij wordt meer inzicht in het fenomeen verworven, worden interventies ontwikkeld en wordt gewerkt aan technische manieren om phishingaanvallen structureel te verstoren. Verder worden opsporingsonderzoeken voorbereid. Naast banken worden ook andere private partijen betrokken; zo is recent contact gelegd met de telecombedrijven en Internet Service Providers. Het project wordt als prioriteit voortgezet in 2020.
In algemene zin geldt dat het strafrecht wordt ingezet in die (fraude)zaken, waarbij die inzet effectief is en er voldoende aanknopingspunten zijn voor opsporing en vervolging. Door de politie en het OM zijn al goede resultaten geboekt. Bij verschillende strafzaken zijn verdachten wegens

[8] https://www.betaalvereniging.nl/actueel/nieuws/aangepaste-uniforme-veiligheidsregels-voor-consumenten.

phishing en de grote maatschappelijke impact daarvan[9] veroordeeld tot hoge gevangenisstraffen en terugbetaling aan slachtoffers. Het cybercrimeteam van de eenheid Zeeland / West Brabant van de politie heeft phishing als kernthema benoemd. Daardoor is ruimte ontstaan voor specialisatie, het genereren van meer inzicht in en overzicht op het fenomeen en het nemen van landelijke regie. Ervaringen worden op landelijk niveau als best practice gedeeld. Ook het Openbaar Ministerie (OM) zet met speciale teams en expertise actief in op de aanpak van phishing en wil de aanval openen op specifieke vormen hiervan, zoals de fraude met betaalverzoeken[10].
Op Europees niveau werken de politie en het OM onder meer mee in het project European Money Mule Action (EMMA). Nederland is samen met Europol en Eurojust «actionleader» (coördinatie door de ECTF in samenwerking met het Parket Noord-Nederland). EMMA bestaat uit een operationele fase waarin internationaal onderzoeken en acties met betrekking tot moneymules worden uitgevoerd en een preventieweek begin december. Ook worden verstoringsmaatregelen onderzocht. Bij dit alles wordt nauw samengewerkt met de banken. In 2019 is EMMA voor de 5^{e} keer uitgevoerd[11].

Misbruik van telecommunicatievoorzieningen

Zoals ik reeds aangaf vindt phishing mede plaats door oneigenlijk gebruik of misbruik van telecommunicatievoorzieningen, waarbij doorgaans telefoonnummers zijn betrokken[12]. Dit is alleen niet het geval als phishing plaatsvindt enkel via internet (websites) of via de inhoud van de communicatie. Meer specifiek, gaat het om de mogelijkheid om tegen relatief lage kosten op grote schaal (via SIM-boxen en databases met al dan niet illegaal verkregen mobiele telefoonnummers), of op kleinere schaal, anoniem of met een valse identiteit telefonische oproepen te plegen of sms-berichten te versturen. De beschikbaarheid en inzet van anonieme prepaid SIM-kaarten draagt bij aan deze problematiek. Via misbruik van het systeem voor nummerdoorgifte kan voorts een niet-toegekend telefoonnummer of het nummer van iemand anders getoond worden als het nummer van de beller/afzender («spoofing»). Een belangrijke ontwikkeling in het gebruik van het systeem van nummerdoorgifte is het gebruik van alfanumerieke tekens (namen). Hierbij wordt de naam van een bedrijf of instantie als identificatie van de afzender, zoals de naam van een bepaalde bank of branche, getoond in plaats van een telefoonnummer. Dit leidt tot extra risico op schade voor consumenten.
Telecomaanbieders spelen een rol bij het aanpakken van misbruik van telecommunicatievoorzieningen, waaronder telefoonnummers[13]. In 2016 is in de Telecommunicatiewet een verbod op spoofing opgenomen. Dit verbod houdt in dat het systeem van nummerdoorgifte niet mag worden gebruikt om onjuiste informatie te verstrekken aan de opgeroepen partij. Deze norm richt zich onder andere tot telecomaanbieders, die daarbij onderling een gedeelde verantwoordelijkheid voor de integriteit van het systeem van nummerdoorgifte hebben. Maatregelen ten behoeve van die

---

[9] Zie onder meer www.rechtspraak.nl (ECLI:NL:RBMNE:2019:5898), https://www.politie.nl/nieuws/2019/december/6/08-aanhouding-betaalfraude.html, https://www.om.nl/actueel/nieuwsberichten/@106322/utrechter/, www.rechtspraak.nl (ECLI:NL:RBZWB:2019:2196), Zie onder meer www.rechtspraak.nl (ECLI:NL:RBDHA:2019:4230).

[10] https://www.ad.nl/rotterdam/het-openbaar-ministerie-opent-de-aanval-op-tikkie-fraudeurs~a4754607b/.

[11] https://sofiaglobe.com/2019/12/04/europol-228-money-mule-recruiters-arrested-in-money-laundering-crackdown/.

[12] Zie ook de antwoorden op de Kamervragen aan de Staatssecretaris van Economische Zaken en Klimaat en de Minister van Justitie en Veiligheid over het voorkomen van wangiri-fraude (26 juni 2018), Aanhangsel Handelingen II 2017/18, nr. 2555.

[13] Idem voetnoot 12.

integriteit zijn van belang in de preventieve aanpak van spoofing en phishing. In de praktijk blijkt het toezicht op dit verbod complex. Dit heeft allereerst te maken met de lange en complexe keten van gebruikers en telecomaanbieders (inclusief aanbieders van zakelijke sms-diensten) die bij nummerdoorgifte zijn betrokken en de hiermee samenhangende vragen rond de verdeling van (juridische) verantwoordelijkheid en technische mogelijkheden. Ook nieuwe marktontwikkelingen, zoals het genoemde gebruik van alfanumerieke tekens in het systeem van nummerweergave, compliceren het toezicht.
De telecomsector onderkent de problematiek en stelt zich actief op om, binnen de hierboven geschetste situatie, maatregelen te nemen. De sector geeft aan dat dit reeds onder meer het onderzoeken van verdachte patronen in in- en uitgaand verkeer en (gericht) informeren van klanten omvat. Het Ministerie van Economische Zaken en Klimaat en de ACM zijn in overleg met de telecomsector, politie, OM en financiële sector over de uitwerking van het spoofingverbod in de praktijk. Hierbij wordt ook gekeken naar mogelijk passende (technische) maatregelen op langere termijn, zoals de inzet van verbeterde authenticatie-technieken. De ACM is daarnaast gestart met een onderzoek naar de integriteit van sms-diensten en de mogelijkheden voor de telecomsector om hinderlijke sms-berichten aan te pakken. Tevens wordt bekeken welke andere instrumenten (naast de bevoegdheden voor handhaving van het spoofingverbod) de ACM als toezichthouder heeft om phishing te voorkomen en de gevolgen te verminderen. Mede afhankelijk van het resultaat van dit onderzoek zal de regelgeving worden aangepast om de effectiviteit van het verbod op spoofing te vergroten. Over de stand van zaken hieromtrent zal uw Kamer in het najaar van 2020 door de Staatssecretaris van Economische Zaken en Klimaat worden geïnformeerd.

Tot slot

De toenemende digitalisering van ons maatschappelijk, economisch en financieel verkeer heeft veel goede kanten, maar kent ook zijn keerzijde: ook criminelen maken hier gebruik van met schade voor mensen, maatschappij en economie. Het voorkomen van fraude, ook van bancaire fraude door middel van phishing, is een zaak van veel verschillende publieke en private partijen en begint bij de oplettendheid van burgers en bedrijven zelf. Ik blijf me mét alle betrokken partijen onverminderd inzetten voor het voorkomen én bestrijden van fraude.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus