Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

29 911 Bestrijding georganiseerde criminaliteit

Nr. 302

BRIEF VAN DE STAATSSECRETARIS VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 16 december 2020

In deze brief informeer ik uw Kamer over de stand van zaken van de aanpak van misbruik van telecommunicatievoorzieningen voor phishing. In de brief van 20 februari 2020[1] heeft de Minister van Justitie en Veiligheid (JenV), mede namens mij, de stand van zaken geschetst omtrent de ontwikkelingen van bancaire fraude door middel van phishing en de aanpak hiervan. Die brief belicht op welke wijze dit probleem wordt aangepakt door publieke en private partijen, waaronder door telecomaanbieders. In de voorliggende brief informeer ik u nader over de aanpak van misbruik van telecommunicatievoorzieningen voor phishing.

Daarbij beschrijf ik eerst kort de problematiek. Vervolgens schets ik het relevante beleidskader (paragraaf 2). De sector heeft op mijn verzoek maatregelen in kaart gebracht waarvan de uitvoering reeds deels heeft aangevangen en op korte termijn zijn verdere beslag krijgt (paragraaf 3). In paragraaf 4 beschrijf ik de (beleids)ontwikkelingen op internationaal niveau die naar verwachting op de langere termijn leiden tot de implementatie van betere authenticatietechnieken.

Daarnaast acht ik aanvullende nationale regelgeving noodzakelijk. Ik bereid hiertoe een wetswijziging voor, die ik naar verwachting rond de zomer van 2021 zal consulteren. Paragraaf 5 gaat nader in op de toezichts- en regelgevingsaspecten.

1. Beschrijving probleem

Phishing is een overkoepelende term voor alle vormen van (financiële) fraude waarbij gegevens van een gebruiker onrechtmatig op afstand worden verkregen. Hierbij worden verschillende kanalen ingezet:

- Phishing via telefoongesprekken;

[1] Kamerstuk 29 911, nr. 273.

kst-29911-302
ISSN 0921 - 7371
's-Gravenhage 2020

- Sms-phishing, waarbij ook alfanumerieke tekens (namen) worden gebruikt als afzenderinformatie;
- Phishing via email;
- Phishing via internetcommunicatietoepassingen zoals Whatsapp en berichtendiensten die worden gebruikt bij online marktplaatsen.

De achtergrond en complexiteit van de problematiek van phishing en daarmee de mogelijkheden voor de aanpak hiervan vanuit het telecomdomein verschillen voor de genoemde communicatiekanalen. Phishing kan plaatsvinden door misleidende informatie op te nemen in de inhoud van de communicatie. Daarnaast spelen de volgende factoren: spoofing, het gebruik van alfanumerieke karakters als afzenderinformatie en het grensoverschrijdende karakter van de betreffende communicatie.

Spoofing

Eén van de bij phishing gebruikte technieken is spoofing, een techniek die wordt gebruikt bij onder meer bancaire fraude en helpdeskfraude. Alhoewel spoofing al jarenlang bestaat lijkt dit fenomeen, nu consumenten steeds meer zijn aangewezen op digitaal contact middels berichtenverkeer, als modus operandi van digitale financiële fraude een steeds grotere rol te spelen.

Spoofing houdt in dat door misbruik van het systeem voor nummerdoorgifte een niet-toegekend nummer, zoals een telefoonnummer, of het nummer van iemand anders getoond wordt als het nummer van de beller/afzender[2] in het adresveld van een oproep of bericht. De fraudeur gebruikt bijvoorbeeld het telefoonnummer van een bank of overheidsinstelling om potentiële slachtoffers mee te bellen.

De achtergrond van de toename van spoofing vormt de voortschrijdende techniek zoals VoIP (Voice over IP) waardoor de mogelijkheden zijn toegenomen om telefoonnummers en andersoortige informatie als afzender op te nemen bij telefonische oproepen en sms-berichten. Hierdoor identificeert een telefoonnummer niet altijd meer de fysieke aansluiting op een netwerk van waaruit wordt gebeld of een bericht wordt gestuurd. Helaas wordt hier ook meer door fraudeurs gebruik van gemaakt, ondanks het bestaande wettelijke verbod op spoofing (zie paragrafen 2 en 5). De integriteit van telecommunicatievoorzieningen in openbare netwerken en eindapparatuur die van invloed zijn op het gebruik van telefoonnummers, speelt in deze context een grote rol bij phishing en spoofing en is van groot belang bij de bestrijding hiervan.

De maatschappelijke, financiële en economische schade door phishing en spoofing treft vele betrokken partijen, waaronder personen die slachtoffer zijn en bedrijven, met name telecomaanbieders, financiële instellingen en overheidsuitvoeringsdiensten. Phishing en spoofing lijken zich in de laatste maanden nog onverminderd te hebben voortgezet. Daarnaast is sprake van een marktontwikkeling waarbij juist telefoonnummers, met name 06-nummers, steeds meer ingezet worden voor authenticatiedoeleinden ook voor toepassingen *buiten het telecomdomein,* zoals tweestapsverificatie waarbij een sms met een code wordt toegestuurd aan de gebruiker. Daarmee wordt de maatschappelijke afhankelijkheid van betrouwbare 06-nummers groter. Sinds enkele jaren is dan ook zowel op nationaal als internationaal niveau een toegenomen inzet zichtbaar bij

[2] Het gaat hierbij om het (telefoon)nummer dat een netwerkaansluitpunt of de gebruiker daarvan identificeert. Internationaal wordt ook de nauwkeurigere term CLI spoofing gebruikt, waarbij CLI staat voor Caller Line Identification.

telecomaanbieders en andere private partijen om de betrouwbaarheid van telefonie als wereldwijd communicatiemedium beter te waarborgen.

Het gebruik van alfanumerieke karakters

Ook anderszins (zonder spoofing in voornoemde zin) kan misleidende afzenderinformatie worden opgenomen of toegevoegd in het adresveld van een oproep of bericht, bijvoorbeeld door het (mede)gebruik van alfanumerieke karakters. Dit laatste is het geval bij sms-phishing waarbij in het adresveld van het bericht alfanumerieke informatie is opgenomen in plaats van een (legitiem) telefoonnummer. Zo kunnen consumenten een sms ontvangen met bijvoorbeeld «Belastingdienst» in plaats van een 06-nummer of shortcode (een viercijferig nummer) in het adresveld.

Grensoverschrijdend verkeer

Het misbruik van telecommunicatievoorzieningen en spoofing heeft een internationale voetafdruk. Afhankelijk van de mate waarin bij de genoemde toepassingen sprake is van telecomverkeer vanuit buiten Nederland en het gebruik van Nederlandse telefoonnummers daarbij door in het buitenland gevestigde entiteiten, wordt de handhaving bemoeilijkt. Bij grensoverschrijdend verkeer kan het gaan om gespoofde nummers van individuele Nederlandse bedrijven die als het oproepende nummer worden weergegeven. Ook kan het gaan om gespoofde landencodes, waarbij de oproep wordt geprofileerd als zijnde afkomstig uit een bepaald land, waaronder Nederland.

2. Beleidskader

De reikwijdte van deze brief omvat het gebruik van telecommunicatievoorzieningen bij phishing. Hieronder vallen vormen van phishing waarbij ook sprake kan zijn van spoofing.

In de Telecommunicatiewet is het wettelijk kader vervat voor het aanbieden en gebruik van het systeem voor nummerdoorgifte. Voor wat betreft spraaktelefonie betreft dit een implementatie van de huidige Universele dienstenrichtlijn[3] (de opvolger van deze richtlijn is het Europees wetboek voor elektronische communicatie (herschikking)- hierna: Telecomcode[4]), die het aanbieden van de nummerweergavefaciliteit voor telefonische oproepen verplicht stelt voor aanbieders van openbare nummergebaseerde interpersoonlijke communicatiediensten. De Telecommunicatiewet stelt in dit verband nadere voorwaarden die gelden voor zowel telefonische oproepen als sms-berichtenverkeer. Op grond van artikel 11.10a is het verboden het systeem voor nummerdoorgifte te gebruiken voor het verstrekken van onjuiste informatie over de beller/afzender bij deze vormen van communicatie (spoofing verbod).

De huidige aanpak van spoofing vanuit het telecomdomein ziet primair op het domein van zogenaamde nummergebaseerde elektronische communicatiediensten. Dit betreft diensten die gebruik maken van nummers die worden toegekend door de overheid en als zodanig worden gereguleerd door de Telecomcode. Van onjuist gebruik van de identificerende functie van een nummer in bestuursrechtelijke zin is sprake als de beller/afzender geen gebruiksrecht over dit nummer heeft. Dit is voor het toezicht complexer als gebruiksrechten en voorwaarden voor het gebruik van nummers voor een communicatiedienst niet worden gereguleerd op grond van een nummerplan.

---

[3] Richtlijn (EG) 2002/22.
[4] Richtlijn (EU) 2018/1972.

In Nederland geeft de ACM nummers uit op grond van door mijn ministerie vastgestelde nummerplannen, voor telefoonnummers betreft dit het Nummerplan telefoon- en ISDN-diensten, en oefent zij toezicht uit op het gebruik van nummers, waaronder in het kader van het spoofing verbod. De door de ACM uitgegeven telefoonnummers worden gebruikt voor spraaktelefonie, data- en sms-verkeer. Indien deze nummers worden gebruikt voor spoofing door een ander dan de nummerhouder, kan de ACM mede in het belang van de nummerhouder in principe eigenstandig optreden tegen diegene of een betrokken telecomaanbieder. Sms shortcodes, alfanumerieke karakters die worden gebruikt voor betaalde of zakelijke sms informatiediensten en emailadressen vallen niet onder een nummerplan. Dit levert voor het toezicht een andersoortige situatie op.

Spoofing vindt ook plaats bij internetcommunicatietoepassingen zoals email. Emailadressen zijn gebonden aan de uitgifte (via registratie) van domeinnamen door private instellingen. Ook het centrale beheer van domeinnamen ligt bij private instellingen, zoals SIDN voor het.nl domein. De registratie van emailadressen, en daarmee de informatie die daarin is opgenomen, is een marktaangelegenheid en gebaseerd op internationale standaarden. Emailadressen worden door aanbieders binnen en buiten Nederland van niet-nummergebaseerde elektronische communicatiediensten en internetcommunicatietoepassingen zoals Gmail, in gebruik gegeven aan Nederlandse eindgebruikers. Dit stelsel van zelfregulering sluit goed aan bij het mondiale beheer van internet.

Van belang is dat voor authenticatietechnieken voor de genoemde internetcommunicatietoepassingen marktstandaarden bestaan die reeds in een volwassen staat van ontwikkeling zijn. In het geval van email worden deze technieken die e-mailspoofing tegengaan in toenemende mate toegepast door Nederlandse en buitenlandse aanbieders van e-maildiensten en gebruikers en daarbij worden deze technieken ook ingebed in standaardsoftware gebruikt door consumenten. Tegelijkertijd zijn er nog te veel aanbieders die achterblijven.

Het stimuleren van de ontwikkeling en het gebruik van goede authenticatietechnieken maakt, naast het algemene gebruik van internetcommunicatiediensten onderdeel uit van mijn bredere beleid op het vlak van het veilige gebruik van ICT. Forum Standaardisatie (waarvan het Ministerie van EZK met het Ministerie van BZK beleidsopdrachtgever is) bevordert het gebruik van deze technieken door overheden, onder andere middels de lijst met voor de overheid verplichte standaarden («pas toe of leg uit»). Platform Internetstandaarden, een publiek-privaat samenwerkingsverband, dat onder meer de testtool Internet.nl aanbiedt, stimuleert de markt om deze technieken toe te passen. Er zijn ondertussen diverse providers met een volledige toepassing van moderne e-mailstandaarden waaronder authenticatietechnieken (100%-score) en dit aantal groeit nog steeds[5].

Ook in het kader van de registratie en uitgifte van.nl domeinnamen zijn initiatieven ontplooid die phishing tegengaan. Zo biedt de SIDN een dienst voor het actief monitoren van registraties van malafide websites, met namen die nauwelijks verschillen van de organisaties die zij nabootsen[6]. Tot de bedoelde initiatieven behoren ook activiteiten van

[5] De mate waarin een website of e-mailadres voldoet aan moderne standaarden kan eenvoudig worden gecheckt via de website Internet.nl. Op deze website is ook een lijst te vinden van grotere en kleinere hosting providers die voor zowel website-ondersteuning als e-mail-ondersteuning een 100%-score hebben. Zie: www.internet.nl/halloffame/hosters.

[6] Bijvoorbeeld de dienst Domeinnaambewakingsservice (DBS), zie https://www.sidn.nl/nieuws-en-blogs/phishing-bestrijden-draait-om-snelheid

SIDN en registrars van.nl domeinnamen om malafide webwinkels aan te pakken[7].

Tenslotte vormen als onderdeel van mijn genoemd bredere ICT-beleid blijvende investeringen van de overheid om consumenten aan te zetten tot bewust veilig digitaal gedrag als reactie op het feit dat Nederlanders steeds meer afhankelijk zijn van het internet voor hun werk en levensbehoeften[8] terwijl de algemene digitale weerbaarheid achterblijft[9]. Hieronder valt ook structurele voorlichting over simpele handelingen. Het publiek-private platform veiliginternetten.nl, waarbij onder andere private partijen als banken en telecomaanbieders zijn aangesloten, speelt hier een belangrijke rol bij.

In het vervolg van deze brief richt ik mij op phishing en spoofing bij telefonie en sms-verkeer.

3. Sectoraanpak

Bij de aanpak van phishing en spoofing in Nederland zijn diverse publieke en private partijen betrokken zoals EZK, de Autoriteit Consument en Markt (ACM), JenV, het Openbaar Ministerie en politie, aanbieders van vaste en mobiele telefonie, aanbieders van sms-diensten en andere private partijen, zoals banken en internetplatforms.

Dit voorjaar heb ik de telecomsector verzocht een gezamenlijk plan van aanpak op te stellen, inclusief tijdspad, voor mogelijke maatregelen vanuit het telecomdomein ten aanzien van phishing en spoofing. De telecomsector, via de Vereniging COIN, en de bancaire sector, via Betaalvereniging Nederland, hebben in het najaar van 2019 toenadering gezocht voor samenwerking bij de aanpak van sms-phishing. Begin 2020 is hiertoe door deze partijen een overleg gestart, aangevuld met EZK, de ACM, politie, Belastingdienst en de financiële sector (hierna kortweg aangeduid als «sector»).

Sms-phishing

Sms-phishing onderscheidt zich van phishing in telefoongesprekken door een andere ketencomplexiteit. De sector constateert dat in Nederland een relatief groot deel van sms-phishing plaatsvindt met een valide (niet gespoofed) 06-nummer als afzender en dat ook een aanzienlijk deel sms-berichten betreft met een alfanumerieke tekst als afzender. In juni 2020 heeft de sector mij een plan van aanpak gezonden. Op basis van een uitgewerkte probleemanalyse presenteert de sector hierin een brede aanpak voor de bestrijding van sms-phishing.

Het genoemde plan van aanpak richt zich op de volgende modi operandi van sms-phishing die elk een aanzienlijke bron hiervan vormen:

- Sms-phishing met een valide 06-nummer als afzender: hierbij wordt gebruik gemaakt van commerciële en technische mogelijkheden om grote aantallen sms-berichten te versturen tegen lage kosten[10];

---

[7] Zie ook mijn kamerbrief inzake consument, data en AI van 4 december 2020 (Kamerstukken 35 134 en 35 251, nr. 14) met reactie op de motie van het lid Palland (CDA) van 15 januari 2020 aan het kabinet te onderzoeken hoe consumenten beter kunnen worden beschermd tegen malafide webwinkels door de huidige aanpak daarvan tegen het licht te houden en te verkennen of aanvullende maatregelen nodig zijn, en daarbij ook het huidige systeem van domeinnaamregistratie te betrekken (Kamerstuk 35 251, nr. 10).

[8] 97% van Nederlanders heeft toegang tot internet in 2019. 87,6% gebruikt dagelijks internet. Zie: https://www.cbs.nl/nl-nl/cijfers/detail/83429NED?dl=27A20.

[9] AlertOnline bewustzijnsonderzoek, 2020.

[10] Veelal met behulp van simboxen.

- Het gebruik van misleidende alfanumerieke informatie (naam van een bekende instelling) als afzender van een sms-bericht. Diverse gespecialiseerde aanbieders van (zakelijke) sms-diensten bieden hiertoe laagdrempelige mogelijkheden.

In het plan van aanpak zijn een aantal mogelijke actielijnen geïdentificeerd met een preventieve of repressieve werking en is een gefaseerde planning vastgesteld voor de uitvoering van deze acties. Het gaat om een palet van acties die liggen op de volgende terreinen:
- Processen en procedures die het delen van kennis- en best-practices tussen de partijen mogelijk maken;
- Het vaststellen van noodzakelijke ketenoverschrijdende operationele maatregelen gericht op het effectief detecteren, stoppen of verstoren van malafide berichtenverkeer, met als onderdeel hiervan het valideren van de afzenderinformatie bij de routering van sms-verkeer;
- Processen die informatie-uitwisseling met politie en de opsporingsmogelijkheden verbeteren.

In de tweede helft van 2020 zijn deze acties en de verantwoordelijkheden van de verschillende partijen hierbij nader verkend en is waar mogelijk reeds (deels) gestart met de implementatie van bepaalde acties. Financiële instellingen zoals banken hebben tevens hun publiekscampagnes voor specifieke doelgroepen geïntensiveerd. Er wordt gewerkt aan een gezamenlijk proces voor het melden van incidenten bij opsporingsdiensten, de inrichting van een meldloket voor gebruikers en het sneller blokkeren van malafide gebruikersaccounts bij financiële instellingen. Daarbij wordt ook onderzocht of en hoe verdachte patronen in sms-verkeer sneller kunnen worden gedetecteerd. Voorts wordt de invoering van een door de betrokken marktpartijen gezamenlijk gebruikt centraal register voor afzenderverificatie bij sms-berichten met een alfanumerieke afzenderinformatie onderzocht. Momenteel onderzoekt de ACM het juridische kader voor de inzet van deze instrumenten en handhaving daarvan, dat van invloed kan zijn op de mogelijke opzet van en medewerking aan dit register (zie paragraaf 5).

Spoofing bij telefonische oproepen

De sector constateert dat in de loop van 2020 is gebleken dat naast sms-phishing ook in toenemende mate sprake is van spoofing van telefoonnummers. Medio 2020 hebben telecomaanbieders, banken en politie een taskforce opgericht die zich specifiek richt op het tegengaan van spoofing van telefoonnummers bij telefonie. Deze taskforce heeft verschillende maatregelen tegen het licht gehouden. Eén daarvan wordt momenteel samen met banken in de praktijk getest in afstemming met de overheid. Deze is erop gericht criminelen te belemmeren consumenten op te lichten via spoofing van specifieke nummers. De eerste resultaten zijn positief en daarom wordt overwogen de maatregelen structureel in te zetten.

Op basis van onderzoek en de genoemde test kan vooralsnog worden afgeleid dat een zeer groot deel van spoofing van telefoonnummers plaatsvindt met telefonieverkeer dat ontspringt in netwerken buiten Nederland. Dit is ook een belangrijk gegeven voor de regulering van het gebruik van telefoonnummers (zie paragraaf 5).

Met het genoemde plan van aanpak en de taskforce spoofing spreken de betrokken sectoren de intentie uit om intensief samen te werken. Ik zie dit, nu ook een start is gemaakt met de uitvoering van voorgestelde maatregelen, als een voortvarende aanpak. Hiermee wordt voorzien in de behoefte om op korte termijn resultaat te behalen. Ik zie daarnaast de

noodzaak om de preventieve werking van de aanpak te versterken. Om dat te bereiken is het voorstel voor het toepassen van afzenderverificatie voor sms-berichten met alfanumerieke afzenderinformatie van belang. Het is nog onduidelijk op welke termijn een effectieve uitvoering daarvan met behulp van een centraal register kan worden gerealiseerd, met dien verstande dat het genoemde onderzoek van de ACM nog loopt en van invloed kan zijn op de mogelijke opzet van en medewerking aan dit register. Daarnaast vormt een belangrijk element voor een voldoende preventieve werking ook de screening van (nieuwe) gebruikers door aanbieders van zakelijke sms-diensten. Deze bieden een laagdrempelige toegang aan meerdere doelgroepen en faciliteren tevens het gebruik van alfanumerieke karakters in de afzenderinformatie. De aanbieders van zakelijke sms-diensten hebben aangegeven dat het gelet op de laagdrempelige toegang van hun dienstverlening lastig is volledig te voorkomen dat via hun diensten malafide sms-verkeer wordt gegenereerd. Over de reikwijdte en uitvoering van de acties en deze genoemde aandachtspunten blijf ik in overleg met de betreffende marktpartijen.

4. Internationale beleidscontext

Zoals eerder gesteld heeft het misbruik van telecommunicatievoorzieningen en spoofing een internationale voetafdruk. Bij grensoverschrijdend verkeer kan het gaan om gespoofde nummers van individuele Nederlandse bedrijven die als het oproepende nummer worden weergegeven. Ook kan het gaan om gespoofde landencodes, waarbij de oproep wordt geprofileerd als zijnde afkomstig uit een bepaald land, waaronder Nederland. Dit heeft gevolgen voor zowel eindgebruikers als telecomaanbieders. Mede gelet op de eerdergenoemde rol van buitenlandse netwerken, kan een effectieve aanpak van spoofing daarom alleen in een internationale context plaatsvinden.

Op mondiaal niveau wordt via de International Telecommunication Union (ITU) aangestuurd op een aanscherping van regels over het toepassen van nummeridentificatie door telecomaanbieders, ter betere bestrijding van spoofing met een focus op grensoverschrijdend telecomverkeer. Op Europees niveau heeft de European Conference of Postal and Telecommunications Administations (CEPT) een aanbeveling uitgebracht met als doel spoofing te bestrijden[11]. De ITU en CEPT hebben daarnaast procedures ontwikkeld voor het bilateraal melden van fraude-incidenten en de behandeling daarvan door de daarbij betrokken landen. De laatste hebben echter in de praktijk nog weinig effect gehad met als achilleshiel de medewerking van landen buiten de EU waar de spoofing plaatsvindt.

Onder invloed van toegenomen fraude gebaseerd op spoofing bij inkomend grensoverschrijdend telefonieverkeer in de VS zijn onder druk van de overheid door private partijen technische standaarden ontwikkeld voor betere authenticatietechnieken voor telefonie[12]. Deze standaarden zijn op nationale basis ontwikkeld maar mogelijk mondiaal toepasbaar. De implementatie van dergelijke authenticatietechnieken is echter technisch en organisatorisch complex en moet voor een telefonische oproep worden ondersteund door alle telecomaanbieders die zijn betrokken bij het afwikkelen van die oproep. Hier zijn dan ook aanzienlijke kosten en een naar verwachting een lange implementatietijd mee gemoeid. Mogelijk komen hier alternatieven bij, voor zowel telefonie als sms, die eenvoudiger en sneller te implementeren zijn. De verwachting is dat de inzet van deze technologieën aanzienlijk kunnen bijdragen aan het bestrijden van

[11] ECC Recommendation (19)03, Measures for increasing Trust in Calling Line Identification and Originating Identification, 21 November 2019.
[12] Dit betreft standaarden/technologieën als STIR/SHAKEN en blockchain.

spoofing. Er is daarom bij de Europese Commissie, het European Telecommunications Standards Institute (ETSI) en het CEPT ook toenemende aandacht voor mogelijke implementatie van dergelijke technieken in Europa. Nederland ondersteunt de betreffende initiatieven.

5. Toezicht en regelgeving

De ACM onderzoekt hoe de voorgestelde maatregelen in het plan van aanpak ter bestrijding van sms-phishing zich verhouden tot de Telecommunicatiewet. De focus ligt daarbij op de rol van de telecomaanbieder, diens zorgplicht om de persoonsgegevens en de persoonlijke levenssfeer van gebruikers te beschermen, in combinatie met een beveiligingsplicht om passende technische maatregelen te nemen ten behoeve van de veiligheid en beveiliging van de door hem aangeboden netwerken en diensten[13]. Tevens zal de ACM onderzoeken (en met de sector bespreken) welke maatregelen in zijn algemeenheid ten aanzien van phishing via telefonie of sms noodzakelijk en proportioneel zijn om de integriteit en veiligheid van telecomdiensten te waarborgen en de persoonlijke levenssfeer van gebruikers van netwerken en diensten te beschermen. Het onderzoek van de ACM ziet ook op gevallen van phishing zonder dat ook sprake is van spoofing.

Vooruitlopend op de uitkomsten van dit onderzoek en eventuele vervolgstappen van de ACM constateer ik dat het wenselijk is het wettelijk kader voor het gebruik van nummers aan te scherpen, waaronder een nadere uitwerking van het verbod op spoofing. De soms lange keten van dienstaanbieders die zijn betrokken bij het routeren van telefonische oproepen en de invloed van de mogelijke manipulatie van afzenderinformatie in telecomverkeer dat vanuit of via het buitenland Nederland binnenkomt, bemoeilijkt de uitvoering van het spoofingverbod. Ook is het wettelijk kader voor nummerdoorgifte als geheel niet toegesneden op innovatie die op dit terrein de laatste jaren heeft plaatsgevonden, waaronder het gebruik van alfanumerieke karakters in de afzenderinformatie.

Om deze redenen ben ik voornemens de regels voor nummerdoorgifte aan te passen en daarbij ook het gebruik van alfanumerieke informatie te betrekken door hieraan passende voorwaarden te verbinden. Deze omvat ook een beperking van het extraterritoriale gebruik van nummers uit het nummerplan. Bij de regels voor nummerdoorgifte zal nadrukkelijk ook de rol van de aanbieder van de telecomdienst van waaruit de oproep plaatsvindt of het bericht wordt gestuurd, worden geadresseerd. Met deze aanpassing zal worden aangesloten bij de eerdergenoemde CEPT-aanbeveling. Mijn voornemen om regelgeving aan te passen, betekent dat de Telecommunicatiewet op een aantal onderdelen op het terrein van het nummerbeleid moet worden gewijzigd en dat lagere regelgeving moet worden opgesteld om een aantal onderdelen van de wet nader in te vullen.

Ik zal naar verwachting rond de zomer van 2021 het desbetreffende wetsvoorstel consulteren.

6. Tot slot

Misbruik van telecommunicatievoorzieningen en spoofing die plaatsvinden in het kader van phishing spelen zich af in een dynamische marktomgeving waarbij veel verschillende partijen zijn betrokken. De aanpak van deze problemen is dan ook complex. De sector heeft met het

[13] Respectievelijk artikel 11.2 en 11.3 van de Telecommunicatiewet.

beschreven plan van aanpak voor sms-phishing en de genoemde taskforce voor spoofing een aanzet gemaakt voor een aantal initiatieven die reeds op korte termijn moeten bijdragen aan het bestrijden van dit misbruik en de gevolgen daarvan. Met nieuwe regelgeving zullen deze initiatieven in de toekomst verder worden ondersteund. De effectiviteit van de maatregelen blijft echter afhankelijk van kwetsbaarheden in de authenticatie van gebruikers en de validatie van de gebruiksrechten van nummers. Daarom ondersteun ik de lange termijn aanpak die loopt via het ETSI en het CEPT om te komen tot geavanceerde authenticatietechnieken.

Ik zal in de komende periode het overleg met de telecomaanbieders continueren. Hierbij zal ik de implementatie van de maatregelen die zijn voorzien in het plan van aanpak en de reikwijdte van deze maatregelen betrekken, in samenhang met de uitkomst van het onderzoek van de ACM. Rond de zomer van 2021 zal ik uw Kamer opnieuw informeren over de stand van zaken.

De Staatssecretaris van Economische Zaken en Klimaat,
M.C.G. Keijzer