Oproep tot kandidaatstelling voor het project Stop phishing via sms

in het kader van het

Nationaal plan voor herstel en veerkracht
As 2 Digitale transformatie

Component 2.1. Cyberveiligheid

Contactpersoon: **Streel Yves** Senior Project Manager

(yves.streel@ccb.belgium.be)

INHOUDSOPGAVE

Inhoudsopgave

1. Context 3
2. Voorwerp en aard van de partnerschapsovereenkomst 3
3. Vereisten 4
3.1. Toegangscriteria 4
3.2. Technische en operationele vereisten 5
3.3. Financiële aspecten 6
3.4. Doelstellingen - verwachte resultaten 6
4. Projectplanning 7
5. Stuurgroep 8
6. Eigendom van de resultaten 8
7. Kandidatuurdossier en engagementen 8
8. Evaluatiecriteria 8
9. Toekenningsmechanisme van subsidies 10
10. Kandidatuur, schema en vertrouwelijkheid 11
Bijlage: kandidatuurformulier 12

1. Context

Cybercriminaliteit is het meest voorkomende economische misdrijf in België, hetzij door het gebruik van phishingdreigingen, malware of via het scannen van netwerken. Bijna twee derde van de Belgische organisaties zijn de afgelopen twee jaar het slachtoffer geweest van economische criminaliteit. De uitdagingen op het vlak van cybersecurity zijn veelzijdig en complementair. Er moet waakzaamheid geboden zijn en de beschermingsinstrumenten en -diensten moeten worden geïmplementeerd. Maar bovenal is het noodzakelijk om onze gegevens te beschermen en de nationale soevereiniteit te waarborgen. Phishing is een grote bedreiging voor de digitale samenleving en een reële rem op het vertrouwen in de digitale economie. Het is immers de meest gebruikte manier voor cybercriminelen om een slachtoffer te misleiden. Phishing heeft vaak ernstige gevolgen voor de slachtoffers, zoals het verlies van privégegevens, toegang tot de rekeningen van het slachtoffer, infectie met een ransomsoftware, financiële fraude, identiteitsdiefstal, indringing in een computersysteem van een bedrijf, ziekenhuis, universiteit of diefstal van intellectuele eigendom.

Phishing is een plaag die in Europa en België voortdurend toeneemt. Op 7 januari 2021 meldde het Centrum voor Cybersecurity België dat "In 2020 meer dan 3,2 miljoen Belgische internetgebruikers phishing hebben gemeld aan suspicious@safeonweb.be (tegenover 1,9 miljoen in 2019). Zo konden 667 356 links naar frauduleuze websites worden geïdentificeerd. "

In het verslag IOCTA 2020 stelt Europol dat "sociale engineering (phishing) een grote bedreiging blijft vormen om andere vormen van cybercriminaliteit te vergemakkelijken. Social engineering en phishing, die gericht zijn op menselijke zwakte in de veiligheidsketen, hebben een grote impact op de samenleving en leiden tot de meeste cybercriminaliteit, gaande van oplichting en afpersing tot de verwerving van gevoelige informatie en de uitvoering van geavanceerde aanvallen op malware".

In zijn rapport "cyberbedreigingslandschap 2020" bevestigde ENISA, het Agentschap van de Europese Unie voor cyberbeveiliging, dat phishing de op twee na grootste bedreiging is en wees het erop dat "er een nieuwe norm zal komen tijdens en na de COVID-19-pandemie, die nog meer zal vertrouwen op een veilige en betrouwbare cyberspace. Het aantal slachtoffers van phishing in de EU blijft toenemen, waarbij kwaadwillende partijen het COVID-19-thema gebruiken om hen aan te trekken. De Business Email Compromise (BEC) en de aanvallen met COVID-19 als thema worden gebruikt door cyberoplichters en zorgen voor een verlies van miljoenen euro's voor EU-burgers en -bedrijven. De Europese, kleine en middelgrote ondernemingen (kmo's) zijn ook het slachtoffer geworden van deze bedreigingen in een tijd waarin velen van hen ernstige financiële moeilijkheden ondervinden als gevolg van inkomensverlies. "

Uitdagingen: phishingberichten die via sms worden verzonden, opsporen en blokkeren voordat ze aan hun slachtoffers worden afgeleverd. Het doel is de nationale veerkracht tegen phishing en fraude via telecommunicatienetwerken te verbeteren om onze burgers, bedrijven en publieke actoren te beschermen.

2. Voorwerp en aard van de partnerschapsovereenkomst

Het Stop Phishing-project heeft tot doel de phishing- en fraudepogingen via telecommunicatienetwerken op te sporen en te blokkeren dankzij de invoering van antiphishing- en antifraudeplatforms bij de Belgische telecomoperatoren, in nauwe samenwerking met het Centrum voor Cybersecurity België en de Belgische telecomregulator (BIPT).

Het Stop Phishing-project is ingedeeld in vier verschillende luiken. Enkel het eerste, nl. het anti-phishing luik voor sms (smishing) komt in onderhavige oproep aan bod. De drie andere luiken, nl. het anti-phishing luik voor email, het anti -fraude platform voor machine gegenereerde telefoonoproepen en voor het opsporen van frauduleuze signaleringsboodschappen in mobiele netwerken zullen later aan bod komen.

Dit project levert zo een aanzienlijke bijdrage aan de digitale transitie door het vertrouwen in de digitale economie te vergroten. Dit vertrouwen versnelt de digitale transitie: burgers gebruiken met een gerust hart de digitale overheidsdiensten en e-commerce; kmo's ontwikkelen hun digitale

transitie en zijn beter beschermd tegen blokkeringsbedreigingen door malware; overheidsdiensten en -besturen zorgen voor veiligere onlinediensten; universiteiten en onderzoekssectoren beschermen hun intellectuele eigendom en de sleutelsectoren zijn beter beschermd tegen de actoren van de dreiging.

Het wettelijk kader om telecomoperatoren in staat te stellen frauduleuze sms (MMS is optioneel) berichten op te sporen en te blokkeren, werd op 31 december 2021 gewijzigd en bekendgemaakt in het Staatsblad.

Onder toezicht van de Stuurgroep coördineren het Centrum voor Cybersecurity België (CCB) en het BIPT de acties met de telecomoperatoren. Het CCB staat voor rekening van de minister van Telecommunicatie in voor het administratief beheer en de opvolging van dit project.

Doelpubliek:

De begunstigden van dit project zijn de volledige Belgische bevolking, de publieke sectoren en de ondernemingen, met inbegrip van de kleine ondernemingen en de zelfstandigen.

Uitvoeringsperiode van het project

Het project zal in januari 2022 van start gaan en zal (uiterlijk) midden 2023 afgerond zijn.

3. Vereisten

3.1. Toegangscriteria

Wie kan deelnemen aan dit project?

Elke operator die wenst deel te nemen aan het Stop sms-phishing project moet:

- actief zijn als mobiele operator op de Belgische markt en conform art. 9 van de WEC aangemeld zijn bij het BIPT;
- in het bezit zijn van minstens 1 operationele sms-C om het sms-verkeer af te leveren aan Belgische mobiele gebruikers;
- de sms- en mms-dienst (optioneel) op de thuismarkt aanbieden;
- een beschrijving kunnen geven van de huidige platforms (uitrusting en interconnectie) en van de bestaande fraudebestrijdingsinstrumenten (bijvoorbeeld firewall);
- wensen te investeren in een nieuw opsporingsplatform van frauduleuze sms (mms is optioneel) berichten.
- Wettelijke vereisten :In zijn aanvraag moet de aanvrager aantonen dat hij alle toepasselijke wetgeving naleeft, onder meer op het vlak van de bescherming van de persoonlijke levenssfeer, in het bijzonder artikel 1251 van de wet betreffende de elektronische communicatie, afgekort "WEC".

[1]"7° wanneer de handelingen worden gesteld door operatoren met als enig doel het bestrijden van fraude gepleegd door middel van berichten die gebruik maken van telefoonnummers zoals sms en mms en onder de volgende voorwaarden:

a) de handelingen blijven beperkt tot het machinaal onderzoeken van de berichten om fraude vast te stellen; een menselijke tussenkomst is uitsluitend toegestaan om de goede werking van de computeralgoritmes te controleren;

b) de operatoren zijn transparant tegenover de eindgebruikers zodat voor hen duidelijk is dat berichten machinaal kunnen worden onderzocht in het kader van fraudebestrijding;

c) de betrokken gegevens mogen alleen worden verwerkt door personen die in opdracht van de operator belast zijn met de fraudebestrijding;

d) de verwerking van de betrokken gegevens blijft beperkt tot de handelingen en de duur die nodig zijn voor de fraudebestrijding of tot het einde van de periode waarin een gerechtelijke betwisting mogelijk is.

"Indien het in het eerste lid, 7°, a), bedoelde onderzoek fraude aantoont, nemen operatoren concrete maatregelen om de fraude te bestrijden, zoals het blokkeren van de berichten of in de berichten het vervangen van URL's die

3.2. Technische en operationele vereisten

De partnerschapskandidaat moet in zijn sollicitatiedossier aantonen dat de voorgestelde oplossing het mogelijk maakt met een zeer hoge mate van betrouwbaarheid een eindscore te bepalen die een betrouwbare indicatie is van de waarschijnlijkheid dat een bericht frauduleus is.

Het algoritme voor de opsporing van frauduleuze berichten moet uit drie elementen bestaan, waarbij aan elk element een score wordt toegekend met een specifieke weging om een eindscore te verkrijgen.

Het gaat om de volgende elementen:

A. Analyse van de sms-inhoud

De aanvrager moet verduidelijken welke methoden worden gebruikt om de inhoud van de malware en de trefwoorden in het tekstbericht te identificeren. Naast de tekst moet ook de aanwezigheid van URL-shortcuts, e-mailadressen, telefoonnummers etc. worden geïdentificeerd.

B. URL-analyse

De aanvrager moet verduidelijken welke methoden worden gebruikt om URL's en de bijbehorende domeinnamen die tot frauduleuze webpagina's leiden, te analyseren, als deze in het bericht zijn opgenomen. Er moet ten minste een betrouwbaarheidsanalyse worden uitgevoerd op basis van onder meer de gebruikte topniveaudomeinnaam, de ouderdom van de domeinnaam en het verschijnen van de domeinnaam op antiphishinglijsten. Er moet ook worden nagegaan of een schadelijk bestand wordt gedownload wanneer de URL wordt opgeroepen. Het platform maakt hiervoor onder meer gebruik van reputatielijsten (URL reputation lists).

C. De analyse van de metagegevens

De aanvrager moet de methoden verduidelijken die worden gebruikt voor de analyse van de metagegevens (telefoonnummer, aantal berichten etc.), wat indicatoren zijn voor frauduleuze berichten.

Deze analyse en de bepaling van de eindscore moeten ook voldoen aan de volgende vereisten van het platform:

1) het platform zal realtime (**Real Time**) functioneren;

2) het platform zal in automatische detectiemodus (**Automatic Detection**) werken, maar sommige manuele interventies van de operator zullen worden aanvaard om de machine learning te verbeteren in de eerste weken van de ingebruikname van het platform;

3) het platform zal berichten in alle talen (**Language Independant**) kunnen verwerken;

4) het platform zal gebruik moeten maken van machine learning met aanpassing van de algoritmen (**Machine Learning**), zodat de prestaties kunnen worden verbeterd via de opgedane en verworven ervaring.

Bovendien moet worden aangegeven hoe valspositieve resultaten kunnen worden voorkomen. De mogelijkheid om een "witte lijst" op te stellen moet worden opgenomen.

Er moet ook worden aangegeven hoe het gemachtigde personeel van de operator een handmatige aanpassing kan uitvoeren op basis van de huidige informatie.

De operator moet vier categorieën definiëren waarin de berichten moeten worden ingedeeld. Elk van deze categorieën komt overeen met een bandbreedte/bereik dat wordt bepaald op basis van de eindscore. De volgende acties kunnen worden ondernomen in functie van de eindscore:

---

doorverwijzen naar een frauduleuze website door een waarschuwingsboodschap of een URL met waarschuwingsboodschap.

Voor 1 februari bezorgen de operatoren het Instituut een jaarlijks verslag waarin minstens aan bod komen de maatregelen die zij het afgelopen jaar genomen hebben om fraude te bestrijden, de effectiviteit ervan alsook de evoluties inzake fraude. "

Categorie	Overeenkomende score (max. 100 - ter indicatie)	Is er sprake van fraude?	Actie
A	>80	Zeker	Bericht wissen
B	>60 en <80	Zeer waarschijnlijk	URL verwijderen
C	>40 en <60	Waarschijnlijk	URL vervangen door waarschuwings-URL
D	> 20 en < 40	Twijfel	Te bepalen actie: bijvoorbeeld een waarschuwing toevoegen aan het bericht (de URL, de tekst of het telefoonnummer niet verwijderen).

De operatoren moeten zich ertoe verbinden om in de mate van het mogelijke een gemeenschappelijke norm voor de indeling in categorieën overeen te komen.

Het algoritme dat wordt gebruikt om de eindscore en de te nemen acties te bepalen, mogen niet leiden tot aanzienlijke vertragingen (behalve in geval van handmatige interventie) bij de distributie van de sms (MMS is optioneel) berichten.

3.3. Financiële aspecten

De kandidaat moet aantonen dat hij gedurende de eerste drie jaar ten minste 50 % van de aankoop- en exploitatiekosten van het platform zal dragen. Daartoe moet de aanvrager alle informatie over de kosten van de dienstverlener verstrekken die hij in het aanvraagdossier heeft opgenomen.

3.4. Doelstellingen - verwachte resultaten

De aanvrager moet een realistisch voorstel indienen voor het verzamelen van statistische gegevens om de doeltreffendheid van de oplossing te meten.

Het doel van het project is om beduidend minder frauduleuze sms (mms is optioneel) berichten te ontvangen van mobiele gebruikers.

Frauduleuze berichten moeten worden opgevat als alle berichten die tot doel hebben de ontvanger (bijvoorbeeld financieel) op oneerlijke of onwettige wijze te schaden, met inbegrip van berichten die bedoeld zijn om malware (al dan niet onrechtstreeks) te installeren.

De modules die de leveranciers voorstellen met als enig doel de SIM-dozen en grijze wegen op te sporen zonder dat eindgebruikers het slachtoffer worden van fraude, kunnen niet worden gesubsidieerd.

De operator zal in zijn antwoord een manier moeten voorstellen om de volgende elementen te meten:

- 1) Het aantal sms'en dat in een bepaalde periode werd geblokkeerd ten opzichte van het totale aantal sms'en in dezelfde periode (rekening houdend met het uitgesloten verkeer). De operatoren zullen moeten aangeven wat het uitgesloten verkeer is.

- 2) Aangezien het platform dat geïmplementeerd zal worden, gebaseerd zal zijn op het principe van automatisch begeleid leren, moeten de fraudeanalisten het algoritme "trainen" door er in de beginfase na de implementatie beslissingen in op te nemen. De operator moet een KPI voorstellen om de gemiddelde tijd per smishingcampagne automatisch te detecteren en te verwerken.

- 3) Wat klachten betreft: de operator moet het "aantal klachten waarvoor geen actie is ondernomen" voor een bepaalde periode vermelden. Dit zijn klachten in verband met smishingcampagnes die niet door het platform werden geïdentificeerd.

- 4) De operator moet cijfers verstrekken om de doeltreffendheid van het platform te meten, aangezien de handmatige analyse van de gegevens tot een minimum wordt beperkt. Dankzij deze maatregelen zal het algoritme de eerste weken/maanden hopelijk nauwkeuriger en efficiënter worden.

- 5) Alle ander relevante cijfers die het platform wekelijks of maandelijks kan voorleggen om aan te tonen dat het platform succesvol opgestart is.

Alle voorgestelde KPI's/maatregelen zullen tijdens de evaluatieperiode worden geëvalueerd (door alle operatoren en de Stuurgroep) en dienen als basis voor de vaststelling van verplichte gemeenschappelijke KPI's die de operatoren na een overeen te komen periode moeten naleven.

Het project zal in elke uitvoeringsfase meetbare resultaten opleveren. We moeten dus niet wachten tot het project is afgerond. De stuurgroep van het project zal een regelmatige evaluatie uitvoeren.

4. Projectplanning

De Belgische telecomoperator zal het "state of the art" antiphishing- en antifraudeplatform in zijn telecommunicatienetwerk implementeren door een projectmatige aanpak te volgen, onder meer:

(1) door de state of art en de meest geavanceerde technieken voor het opsporen en blokkeren van frauduleuze sms-berichten te evalueren;

(2) door de markt te beoordelen en de leverancier te selecteren;

(3) door de geselecteerde oplossing te implementeren;

(4) door dit platform te gebruiken en de resultaten te evalueren.

De operatoren moeten een gedetailleerd uitvoeringsplan delen dat alle fasen van het project omvat; het project moet de volgende fasen dekken:

- oproep tot kandidaten (RFP)
- evaluatie van de antwoorden
- selectie van een of twee kandidaten
- test van de gekozen oplossing(en) (PoC)
- selectie van de eindoplossing
- definitie van het einddesign
- implementatie
- validering in testomgeving (beperkt verkeer)
- evaluatie
- in productie brengen

5. Stuurgroep

De Stuurgroep bestaat uit:

- **de minister van Telecommunicatie**, vertegenwoordigd door de heer Gertjan Boulet;
- **het BIPT**, vertegenwoordigd door de heer Jan Vannieuwenhuyse;
- **het CCB**, vertegenwoordigd door de heer Miguel de Bruycker,mevrouw Phédra Clouner en **de projectleider**: Yves Streel;

De Stuurgroep komt samen om de verschillende fasen van het project te valideren en te evalueren, met inachtneming van de *milestones* die in overleg met de operatoren worden vastgesteld.

6. Eigendom van de resultaten

Elke operator moet de behaalde resultaten dankzij de implementatie van dit nieuwe platform in alle fasen van het project, alsook een maandelijks verslag vanaf de officiële lancering delen om het rendement van de investering in de komende maanden en jaren te kunnen evalueren.

De precieze gegevens en modaliteiten van de verdeling (type informatie, granulariteit en eenheid) zullen worden bepaald door de Stuurgroep en de operatoren tijdens het project, na selectie van de door de operator gekozen oplossing.

7. Kandidatuurdossier en engagementen

De kandidaat moet in zijn kandidatuurdossier aantonen dat hij of, in voorkomend geval, dat de beoogde leverancier voldoet aan alle criteria beschreven in hoofdstuk 3.1.

Daarnaast moet de kandidaat een gedetailleerde beschrijving geven van de SMS (MMS is optioneel) systemen (functioneel en architecturaal) waarover hij op 1 april 2022 beschikt. Ook moet een volledige beschrijving van de bestaande firewall en de antifraudesystemen worden verstrekt.

De kandidaat moet beschrijven hoe hij zal voldoen aan de criteria die worden voorgesteld in 3.2 (technische en operationele vereisten), 3.1 (wettelijke vereisten) en 3.3 (financiële aspecten).

De kandidaat moet bijkomende elementen verstrekken die hij belangrijk acht om het doel van het project te bereiken en die de deskundigheid van de kandidaat en in voorkomend geval van de beoogde leverancier aantonen (bijvoorbeeld uitvoeringen in het buitenland).

De kandidaat moet een gedetailleerd projectplan indienen om het antifraudesysteem volledig operationeel te maken.

De operator wordt ook verzocht om in het kader van dit project één enkel contactpunt aan te duiden.

De kandidaat moet zich ertoe verbinden wekelijks samen met de projectleider de stand van zaken van zijn project te verstrekken.

8. Evaluatiecriteria

Een operator die niet voldoet aan een of meerdere toegangscriteria (zie hoofdstuk 3.1) kan niet deelnemen aan het project.

Om in aanmerking te komen voor een evaluatie van zijn dossier moet de operator volledig voldoen aan de vereisten en verbintenissen (zie hoofdstuk 7).

Op basis van de verstrekte antwoorden zullen de kandidaturen worden beoordeeld, waarbij de aanvrager ten minste 60 punten op 100 moet behalen om in aanmerking te komen voor subsidies volgens het volgende schema:

a. Technische en operationele vereisten: 60 punten

De evaluatie zal gebeuren volgens de volgende toekenningsregels:

Criteria	**Punten**
Realtime platform	5
Automatic detection	5
Language independant	5
Machine Learning	5
Mogelijkheid tot handmatige interventie	5
Analyse van de sms-inhoud	5
URL-analyse	5
Analyse van de metagegevens	5
Gebruik van een algoritme voor de opsporing van frauduleuze tekstberichten	10
Gedetailleerde beschrijving van de beslissingsmatrix	10

b. Financiële aspecten: 20 punten.

De evaluatie zal gebeuren volgens de volgende toekenningsregels:

Criteria	**Punten**
Gedetailleerde presentatie van alle projectkosten over een periode van drie jaar	20

c. Statische verslagen en informatie: 20 punten.

De evaluatie zal gebeuren volgens de volgende toekenningsregels (uitleg over de te verstrekken informatie zie hoofdstuk 3):

Criteria	**Punten**
Verslag 1: Het aantal sms'en dat in een bepaalde periode werd geblokkeerd ten opzichte van het totale aantal sms'en in dezelfde periode (rekening houdend met het uitgesloten verkeer)	3
Verslag 2: KPI om de gemiddelde tijd per smishingcampagne automatisch te detecteren en te verwerken	3
Verslag 3: het "aantal klachten waarvoor geen actie is ondernomen" voor een bepaalde periode	3
Verslag 4: meten van de efficiëntie van het platform	6
Verslag 5: relevant cijfer dat het platform wekelijks of maandelijks kan voorleggen om aan te donen dat het platform succesvol is opgestart	5

In een latere fase zal de kandidaat, indien hij geselecteerd wordt, met de minister onderhandelen om een partnerschapsovereenkomst te sluiten. Pas na het sluiten van een dergelijke overeenkomst kan de aanvrager subsidies krijgen (zie volgend hoofdstuk).

9. Toekenningsmechanisme van subsidies

In het kader van haar begroting beschikt de federale regering over een geschatte maximumenveloppe van 2 295 000 € voor de uitvoering van dit project met de verschillende, geselecteerde telecomoperatoren.

Binnen de hierboven aangegeven budgettaire grenzen zal de federale staat maximaal 50% financieren van de totale kosten voor de investeringen, de uitvoering en de exploitatie van elk antiphishing- en antifraudeplatform via sms voor de jaren 2022-2023-2024. De resterende 50% of meer blijft ten laste van elke telecomoperator.

In het kandidatuurdossier moet elke operator alle uitgesplitste en in detail aangetoonde kosten vermelden (zie hoofdstuk 4.3). De operator moet met andere woorden de totale kostprijs vermelden voor de oprichting van zijn platform en de uitsplitsing over de verschillende jaren 2022-2023-2024 voor elk type uitgave (software, hardware, personeel, onderhoud en anderen).

De totale tussenkomst bedraagt dus maximum 50% van de totale kostprijs van het project voor de jaren 2022-2024. De door de federale staat verstrekte subsidies zullen evenwel gebruikt moeten worden voor de uitgaven die de operatoren in 2022, en in voorkomend geval in 2023, hebben gedaan en moeten door bewijsstukken worden gestaafd (zie verder).

De subsidies kunnen alle aspecten/kosten van het project dekken. De middelen zullen aan de telecomoperator worden toegewezen op basis van de gegevens over de kosten van het project (investeringen, uitvoering en exploitatie) die door de operatoren worden verstrekt op het moment dat aan de vraag wordt voldaan.

Indien 50% van de totale kosten van de gekozen kandidaturen hoger blijkt te zijn dan het voorziene totale budget, wordt een verdeelsleutel toegepast voor de verdeling van de subsidies tussen de telecomoperatoren: elke geselecteerde kandidaat ontvangt een deel van de subsidies naar rato van het aantal op zijn netwerk actieve simkaarten gedeeld door het totaal aantal actieve simkaarten van alle deelnemers (met referentiedatum op 31 december 2021 en betekend aan het BIPT overeenkomstig artikel 137 van de wet van 13 juni 2005 betreffende de elektronische communicatie en artikel 14, § 2, 2° van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector. Actieve simkaarten voor datacommunicatie en IoT (M2M) worden uitgesloten.

De fondsen zullen op basis van het volgende principe worden toegekend:

1/ **Betaling 1**: voorfinanciering van 40% van de totale subsidie die na ondertekening van het protocolakkoord wordt aanvaard

2/ **Betaling 2**: financiering van 40% van de totale subsidie die wordt aanvaard voor de ingebruikneming van het platform

3/ **Betaling 3**: financiering van de resterende 20% aan het einde van het project, zodra kan worden aangetoond dat het platform volledig aan de verwachte resultaten voldoet (zie hoofdstuk 3).

De uitwerking van de subsidies zal voorwerp uitmaken van een toelagebesluit (Koninklijk Besluit) en protocol met de Minister van Telecommunicatie.. Ze kunnen worden uitbetaald in 2022 en 2023.

Om de overschrijvingen van de tweede en de derde betaling uit te voeren, zullen de operatoren worden verzocht alle nodige bewijsstukken over te leggen. Dit deel zal worden beschreven in het te ondertekenen protocolakkoord.

De subsidies mogen niet worden gebruikt voor andere doeleinden dan de aanpassingen die nodig zijn voor de uitvoering van het antifraudeplatform.

10. Kandidatuur, schema en vertrouwelijkheid

Het project zal in januari 2022 van start gaan en moet (ten laatste) midden 2023 afgerond zijn.

De kandidaturen worden ingediend via het formulier in bijlage en moeten alle in deze oproep tot kandidaturen vermelde informatie bevatten en **uiterlijk op 13 mei 2022** worden ingediend.

De antwoorden zullen naar de projectleider worden gestuurd: Yves Streel

Via e-mail yves.streel@ccb.belgium.be

Alle informatie die door de kandidaat wordt verstrekt, zal door het BIPT, het CCB en de minister van Telecommunicatie of haar beleidscel in de meest strikte vertrouwelijkheid worden behandeld.

Petra De Sutter (Signature)

Digitaal ondertekend door Petra De Sutter (Signature)
Datum: 2022.03.31 15:55:17 +02'00'

Vice-eersteminister Petra De Sutter

Bijlage: kandidatuurformulier

1. Toegangscriteria

Criteria	Ja/ Nee	Bewijs
Actief als mobiele operator op de Belgische markt en conform art. 9 van de WEC aangemeld zijn bij het BIPT		
In het bezit zijn van minstens 1 operationele sms-C om het sms-verkeer af te leveren aan Belgische mobiele gebruikers		
De SMS-dienst aanbieden op de interne markt		
Beschrijving van de bestaande platforms (uitrusting en interconnectie) en van de bestaande fraudebestrijdingsinstrumenten (bijvoorbeeld: firewall)		
Wensen te investeren in een nieuw opsporingsplatform van frauduleuze sms		
Alle toepasselijke wetgeving naleeft, onder meer op het vlak van de bescherming van de persoonlijke levenssfeer, in het bijzonder artikel 125[2] van de wet betreffende de elektronische communicatie, afgekort "WEC".		
Rekening houden met MMS-berichten		

2. Technische en operationele vereisten: 60 punten.

Criteria	Ja/ Nee	Bewijs
Real-time platform		
Automatic detection		
Language independant		
Machine Learning		
Mogelijkheid tot handmatige interventie		
Analyse van de sms-inhoud		
URL-analyse		
Analyse van de metagegevens		
Gebruik van een algoritme voor de opsporing van frauduleuze tekstberichten		
Gedetailleerde beschrijving van de beslissingsmatrix		

3. Financiële aspecten: 20 punten.

Criteria	Ja/ Nee	Bewijs
Gedetailleerde presentatie van alle projectkosten over een periode van drie jaar		

4. Doelstellingen - verwachte resultaten (Statische verslagen en informatie)**: 20 punten.**

Criteria	**Ja/ Nee**	**Bewijs**
Verslag 1: Het aantal sms'en dat in een bepaalde periode werd geblokkeerd ten opzichte van het totale aantal sms'en in dezelfde periode (rekening houdend met het uitgesloten verkeer)		
Verslag 2: KPI om de gemiddelde tijd per smishingcampagne automatisch te detecteren en te verwerken		
Verslag 3: het "aantal klachten waarvoor geen actie is ondernomen" voor een bepaalde periode		
Verslag 4: meten van de efficiëntie van het platform		
Verslag 5: relevant cijfer dat het platform wekelijks of maandelijks kan voorleggen om aan te tonen dat het platform succesvol is opgestart		

5. Andere vereiste informatie.

Criteria	**Ja/ Nee**	**Bewijs**
Gedetailleerd projectplan (met alle fasen) om het antifraudesysteem volledig operationeel te maken		
Alle uitgesplitste en in detail aangetoonde kosten (zie hoofdstuk 4.3), d.w.z. een beschrijving van de totale kostprijs voor de oprichting van het platform en de uitsplitsing over de verschillende jaren 2022-2023-2024 voor elke soort uitgave		
Alle belangrijke bijkomende elementen om het doel van het project te bereiken en die de deskundigheid van de kandidaat en in voorkomend geval van de beoogde leverancier aan te tonen (bijvoorbeeld uitvoeringen in het buitenland)		
Eén contactpunt in het kader van dit project		
verbindt zich ertoe om wekelijks samen met de projectleider de stand van zaken van zijn project te verstrekken.		