Oproep tot kandidaatstelling voor het project Stop phishing via e-mail

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

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. In 2021 werden er 4.500.000 berichten doorgestuurd naar verdacht@safeonweb.be. In 2022 groeit dit aantal nog steeds: we hebben meer dan 5,5 miljoen berichten ontvangen en konden we 1,5 miljoen verdachte URL's detecteren. Dat betekent dat we dagelijks gemiddeld 15.000 berichten verwerken.

In het verslag IOCTA 2020 stelt Europol dat "social engineering (phishing) een grote bedreiging blijft vormen om andere vormen van cybercriminaliteit te vergemakkelijken. Social engineering en phishing, die gericht zijn op de menselijke zwakte in de veiligheidsketen, hebben een aanzienlijke 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 "Cyber Threat Landscape 2022" bevestigde ENISA, het Europees Agentschap voor Netwerk- en Informatiebeveiliging, dat phishing het meest gebruikte middel is om een eerste intrede in een organisatie te maken. Social engineering, en in het bijzonder phishing, blijft een populaire techniek voor aanvallers om hun kwaadaardige activiteiten uit te voeren. Europese kleine en middelgrote ondernemingen (kmo's) zijn ook het slachtoffer geworden van deze bedreigingen terwijl vele van hen op dit moment ernstige financiële moeilijkheden ondervinden als gevolg van de COVID-19-crisis en de huidige energiecrisis. "

Uitdagingen: Phishingberichten die via e-mail 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 fraudebestrijdingsplatformen bij de Belgische telecomkandidaten en internetproviders, in nauwe samenwerking met het Centrum voor Cybersecurity België en de Belgische telecomregulator (BIPT).

Het Stop Phishing-project bestaat uit vier verschillende delen. De implementatie van het eerste deel, antiphishing voor sms (smishing), loopt momenteel. Het tweede deel gaat in op antiphishing per e-mail en wordt in deze oproep aangekaart. De andere twee delen, namelijk het fraudebestrijdingsplatform voor telefoongesprekken door machines en het fraudebestrijdingsplatform voor de opsporing van frauduleuze meldingsberichten in mobiele netwerken, zullen later worden besproken.

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.

Onder toezicht van de Stuurgroep coördineren het Centrum voor Cybersecurity België (CCB) en het BIPT de acties met de telecomkandidaten. 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 personen die een e-mailadres hebben dat wordt aangeboden en beheerd door een telecomkandidaat of internetprovider die een internettoegangsdienst aanbiedt op het Belgische grondgebied.

Uitvoeringsperiode van het project

Het project zal begin 2023 van start gaan met de oproep tot kandidaatstelling en moet op het einde van het eerste kwartaal van 2024 afgerond zijn.

3. Vereisten

3.1. Toelaatbaarheidscriteria

Wie kan er deelnemen aan dit project?

Elke kandidaat of internetprovider die wenst deel te nemen aan het Stop Phishing-project via e-mail moet:

- actief zijn als kandidaat of internetprovider op de Belgische markt en conform art. 9 van de WEC: Wet van 13 juni 2005 betreffende de elektronische communicatie aangemeld zijn bij het BIPT;
- de maildienst op de interne markt aanbieden aan de burgers via een privé- of bedrijfsadres;
- over minstens één operationele e-mail Gateway beschikken om het mailverkeer bij de gebruikers af te leveren;
- een beschrijiving geven van de bestaande platforms (uitrusting en interconnectie) en van de bestaande statische/reactieve en dynamische/proactieve fraudebestrijdingstools (zie paragraaf 3.2) om phishing via e-mail te bestrijden.
- ervoor openstaan om te investeren in een nieuw platform voor het opsporen van frauduleuze e-mails of in de uitbreiding door nieuwe functionaliteiten van hun huidige platform toe te voegen om de opsporing ervan te verbeteren;
- indien de kandidaat op het moment van de indiening al de analyse van de verschillende oplossingen heeft uitgevoerd en de test van een potentiële oplossing uitvoert, bijvoorbeeld door middel van een grootschalig proefproject, zal hij dit in zijn kandidatuur verduidelijken. Dit heeft geen invloed op de toelaatbaarheid van het project.
- De aanvrager moet aantonen dat hij alle geldende wetgeving naleeft, met name op het gebied van de privacybescherming.
- De aanvrager moet een realistisch voorstel indienen voor het verzamelen van statistische gegevens om de doeltreffendheid van de oplossing te meten.

3.2. Technische en operationele vereisten

De operatoren en internetproviders die de maildienst aanbieden, hebben al oplossingen, maar deze zijn nog steeds ontoereikend ten opzichte van de vindingrijkheid van de cybercriminelen. Deze oproep tot kandidaatstelling beantwoordt aan de wens om de e-mailfraudebestrijdingssystemen doeltreffend en significant te verbeteren door gebruik te maken van de nieuwste technieken die door de deskundige leveranciers worden voorgesteld.

Momenteel zijn er twee soorten systemen:

- <u>Statisch (reactief):</u>

- maakt het mogelijk (alleen) gekende phishingcampagnes reactief op te sporen
- gebaseerd op vingerafdrukken (fingerprints) / indicatoren van een gecompromitteerd systeem (IoCs-Indicators of Compromise) / hashingresultaten (hashes) etc.
- gebruikt enkel gekende lijsten (van domeinen/adressen etc.) en vooraf verstrekte externe reputatiescores en probeert geen soortgelijke clusters van berichten met kleine variaties te onthullen

- <u>Dynamisch (proactief):</u>

Het voorziet in een onmiddellijke opsporing van

- nieuwe phishingcampagnes en inhoudelijke variatie
- dynamische reputatiescores gebaseerd op overeenkomsten tussen berichten (inhoud/metagegevens)

Het nieuwe systeem moet in staat zijn om nieuwe en tot dan toe ongekende phishingcampagnes autonoom op te sporen, waarbij gebruik wordt gemaakt van de meest geavanceerde technieken,

ontworpen door artificiële intelligentie, met gebruik van alle of een deel van de volgende technieken:

o Gedragsgebaseerde aanpak (Behavioral based approach)

o Heuristische gedragsanalyse (Heuristic based behavioral analysis)

o Automatische leeralgoritmen (Machine learning algorithms)

o Vision-analyse en -techniek via de computer (Computer Vision)

Het algoritme voor de opsporing van frauduleuze berichten moet gebaseerd zijn op de analyse van de volgende elementen:

A. Analyse van het e-mailadres van de verzender

De aanvrager moet verduidelijken welke methoden worden gebruikt om de afzender van het bericht te identificeren en te analyseren.

B. Analyse van het IP-adres

De aanvrager moet verduidelijken welke methoden worden gebruikt om het IP-adres van de verzender te identificeren en te analyseren.

C. Analyse van de mailinhoud

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.

D. 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 URL-reputatielijsten (URL reputation lists).

E. De analyse van de metagegevens

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

F. De analyse van de bijlagen

De aanvrager moet verduidelijken welke methoden worden gebruikt voor de analyse van de bijlagen (pdf-bestand, word-bestand, archiefbestand etc.) wat indicatoren zijn voor frauduleuze berichten.

G. De analyse van afbeeldingen

De aanvrager moet verduidelijken welke methoden worden gebruikt voor de analyse van afbeeldingen (QR-code, afbeelding gebaseerd op tekst en logo), wat indicatoren zijn voor frauduleuze berichten.

Deze analyses moeten ook voldoen aan de volgende eisen van het platform:

1) het platform zal in realtime (**Real Time**) werken, de dynamische tellers en de reputatiescores zullen worden berekend door de oplossing, in de plaats van een statisch systeem (reactief) via lijsten (van gekende domeinen en adressen etc.) en externe reputatiescores die vooraf zijn verstrekt;

2) het platform zal in automatische detectiemodus (**Automatic Detection**) werken, maar sommige manuele interventies van de kandidaat 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;

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

De kandidaat moet drie 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:

Categorie	Overeenkomende score (max. 100 - ter indicatie)	Is er sprake van fraude?	Actie
A	>80	Zeker	Bericht wissen (en aldus niet afleveren aan eindgebruiker)
B	>40 en <80	Waarschijnlijk	Het bericht in de map "Ongewenste e-mail" of "spam" plaatsen en een duidelijke waarschuwing toevoegen aan het onderwerp van het bericht
C	>20 en <40	Twijfel	Het bericht in de map "Postvak IN" plaatsen met verwittiging "gevaar"

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 verspreiding van e-mails.

De gedetailleerde informatie die is verzameld na de verschillende analyses (scan) zoals hierboven beschreven, moet zo snel mogelijk worden vernietigd. Dit sluit uiteraard niet uit dat op basis van de scan statistische informatie in geaggregeerde vorm wordt bijgehouden om het algoritme te voeden.

De kandidaat voor het partnerschap moet in diens kandidatuurdossier aantonen dat de voorgestelde oplossing een doeltreffende bestrijding van phishing via e-mail mogelijk maakt.

3.3. Financiële aspecten

De kandidaat moet aantonen dat hij ten minste 50% van de kosten voor de aankoop en het gebruik van het nieuwe systeem (nieuw platform of uitbreiding van de functionaliteiten) dat gedurende de eerste drie jaar wordt ingevoerd, voor diens rekening neemt. Daartoe moet de aanvrager alle informatie over de kosten van de dienstverlener verstrekken die hij in het aanvraagdossier heeft opgenomen. In het kandidatuurdossier moet elke kandidaat alle uitgesplitste en in detail aangetoonde kosten vermelden. De kandidaat moet met andere woorden de totale kostprijs vermelden voor de oprichting en het gebruik van diensplatform gedurende drie jaar, opgesplitst over de verschillende jaren 2023-2024-2025-2026 voor elk type uitgave (software, hardware, personeel, onderhoud en andere).

3.4. Projectplanning

De Belgische telecomoperator of de internetprovider zal het "state of the art" antiphishing- en fraudebestrijdingsplatform in zijn netwerk implementeren door een projectmatige aanpak te volgen, met name:

(1) door de "state of the art" en de meest geavanceerde technieken voor het opsporen en blokkeren van frauduleuze e-mails 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 kandidaten moeten een **gedetailleerd implementatieplan** delen dat alle fasen van het project omvat, van definitie tot implementatie alsook de volledige exploitatie ervan.

3.5. Doelstellingen - verwachte resultaten (Informatie en statistische verslagen)

Het project heeft als doel om de gebruikers beduidend minder frauduleuze e-mails te laten ontvangen.

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 kandidaat zal in diens antwoord een manier moeten voorstellen om de volgende elementen te meten:

- 1) Het aantal e-mails dat in een bepaalde periode werd geblokkeerd ten opzichte van het totale aantal e-mails in dezelfde periode (rekening houdend met het uitgesloten verkeer). De kandidaten 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 fraudanalisten het algoritme "trainen" door er in de beginfase na de implementatie beslissingen in op te nemen. De kandidaat moet een KPI voorstellen om de gemiddelde tijd per phishingcampagne automatisch te detecteren en te verwerken.

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

- 4) De kandidaat 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 andere 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 beoordeeld (door alle kandidaten en de Stuurgroep) en dienen als basis voor de vaststelling van verplichte gemeenschappelijke KPI's die de kandidaten na een overeen te komen periode moeten naleven.

Het project levert meetbare resultaten op vanaf de lancering van het platform en de stuurgroep van het project voert een regelmatige evaluatie uit.

4. 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 en 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 geselecteerdenworden vastgesteld.

5. Eigendom van de resultaten

Elke geselecteerde moet de behaalde resultaten dankzij de implementatie van dit nieuwe platform in alle fasen van het project delen, alsook een maandelijks verslag vanaf de officiële lancering 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 kandidaten tijdens het project, na selectie van de door de kandidaat gekozen oplossing.

6. Kandidatuurdossier

De kandidaat moet een kandidatuurdossier indienen (zie bijlage).

De kandidaat moet in dit kandidatuurdossier aantonen dat hij voldoet aan alle in hoofdstuk 3.1 beschreven toelaatbaarheidscriteria.

Daarnaast moet de kandidaat een gedetailleerde beschrijving geven van de e-mailsystemen (functioneel en architecturaal) waarover hij op 1 december 2022 beschikt. Er moet ook een beschrijving worden verstrekt van de bestaande statische en/of dynamische fraudebestrijdingssystemen voor e-mail (zie paragraaf 3.2).

De kandidaat moet beschrijven hoe hij zal voldoen aan de criteria die worden voorgesteld in 3.2 (technische en operationele vereisten), 3.3 (financiële aspecten), 3.4 (Projectplanning) en 3.5 (verwachte resultaten).

De kandidaat moet een gedetailleerd projectplan (3.4) indienen om het fraudebestrijdingssysteem volledig operationeel te maken.

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 aan te tonen (bijvoorbeeld uitvoeringen in het buitenland) te verstrekken.

De kandidaat 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.

7. Evaluatiecriteria

Opdat diens kandidatuur kan worden geëvalueerd, moet de kandidaat voldoen aan alle vereisten en engagementen (zie hoofdstuk 6).

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**
Real-Time platform	3
Automatic detection	3
Language independant	3
Behavioral based approach	3
Heuristic based behavioral analysis	3
Machine Learning	3
Computer Vision	3
Analyse van het adres van de afzender	4
Analyse van het IP-adres	4
Analyse van de mailinhoud	4
Analyse van de bijlagen (pdf- en word-bestand, archiefbestand)	4
Analyse van de URL('s)	4
Analyse van de afbeeldingen (QR-code, afbeelding gebaseerd op de tekst en het logo)	4
Analyse van de metagegevens	4
Gebruik van een algoritme voor de opsporing van frauduleuze berichten	4
Gedetailleerde beschrijving van de beslissingsmatrix	4
Mogelijkheid tot handmatige interventie	3

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. Projectaspecten: 10 punten

De evaluatie zal gebeuren volgens de volgende toekenningsregels:

Criteria	**Punten**
Presentatie van een gedetailleerd projectplan om het fraudebestrijdingssysteem volledig operationeel te maken.	10

d. Statische verslagen en informatie: 10 punten

Wat hier zal worden geëvalueerd, is de manier waarop het rapport is ontwikkeld en het formaat ervan. De evaluatie zal gebeuren volgens de volgende toekenningsregels:

Criteria	**Punten**
Verslag 1: Het aantal mailS dat in een bepaalde periode werd geblokkeerd ten opzichte van het totale aantal mailS in dezelfde periode (rekening houdend met het uitgesloten verkeer)	2
Verslag 2: KPI om de gemiddelde tijd per phishingcampagne voor mailverkeer automatisch te detecteren en te verwerken	2

Verslag 3: het "aantal klachten waarvoor geen actie is ondernomen" voor een bepaalde periode	2
Verslag 4: meten van de efficiëntie van het platform	2
Verslag 5: relevant cijfer dat het platform wekelijks of maandelijks kan voorleggen om aan te tonen dat het platform succesvol is opgestart	2

In een latere fase zal er met de kandidaat, indien hij geselecteerd wordt, een protocolakkoord worden gesloten. Pas na het sluiten van een dergelijke overeenkomst kan de kandidaat subsidies krijgen (zie volgend hoofdstuk).

8. Toekenningsmechanisme van subsidies

In het kader van haar begroting beschikt de federale regering over een maximumenveloppe die geraamd wordt op: 2 992 500 euro voor de uitvoering van dit project met de verschillende kandidaten die zullen worden geselecteerd.

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 fraudebestrijdingsplatform via e-mail voor de jaren 2023-2024-2025-2026. De resterende 50% of meer blijft ten laste van elke telecomkandidaat.

De totale tussenkomst bedraagt dus maximum 50% van de totale kostprijs van het project voor de jaren 2023-2026. De door de federale staat verstrekte subsidies zullen evenwel gebruikt moeten worden voor de uitgaven die de kandidaat in 2023 en 2024 hebben gedaan en moeten door bewijsstukken worden gestaafd (zie verder).

De subsidies kunnen alle aspecten/kosten van het project dekken. De middelen zullen worden toegewezen aan de Belgische telecomoperator of internetprovider op basis van de projectkostengegevens (investeringen, uitvoering en exploitatie) die in het kandidatuurdossier worden verstrekt.

Indien 50% van de totale kosten van de geselecteerde kandidaturen hoger blijkt te zijn dan het voorziene totale budget, wordt een verdeelsleutel toegepast voor de verdeling van de subsidies tussen de geselecteerde kandidaten: elke geselecteerde kandidaat zal een deel van de subsidies ontvangen in verhouding tot het aantal breedbandaansluitingen en het totaal aantal breedbandaansluitingen van alle geselecteerde partijen op 1 januari 2023.

De compensatie voor de openbare dienst wordt als volgt vrijgegeven:

- een eerste schijf van 40% van de in aanmerking komende kosten na de sluiting van het protocol;

- een tweede schijf van 40% van de in aanmerking komende kosten voor de ingebruikname van het platform voor e-mails;

- een derde schijf waarvan het bedrag overeenstemt met 50% van de werkelijke in aanmerking komende kosten min het bedrag dat reeds betaald werd in de eerste en tweede schijf, wanneer de kandidaat aantoont dat het blokkeerplatform voor e-mails volledig beantwoordt aan de verwachte resultaten zoals beschreven in het protocol en uiterlijk op 31 maart 2024.

De uitwerking van de subsidies zal het voorwerp uitmaken van een beslissing tot toekenning (koninklijk besluit) en van een protocolakkoord met de minister van Telecommunicatie. Ze kunnen worden uitbetaald in 2023 en 2024.

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

De subsidies mogen niet gebruikt worden voor andere doeleinden dan de nodige aanpassingen voor de implementatie van het nieuwe fraudebestrijdingsplatform of de uitbreiding van het huidige platform zoals bepaald in hoofdstuk 3.

9. Kandidatuur, schema en vertrouwelijkheid

De kandidaturen worden ingediend via het formulier in bijlage. Ze moeten alle in deze oproep tot kandidaturen vermelde informatie bevatten en uiterlijk op 24 maart 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.

Vice-eersteminister Petra De Sutter

Bijlage: kandidatuurformulier

1. Toelaatbaarheidscriteria

Criteria	Ja/ Nee	Bewijs
Actief zijn als kandidaat of internetprovider op de Belgische markt en conform art. 9 van de WEC: Wet van 13 juni 2005 betreffende de elektronische communicatie aangemeld zijn bij het BIPT		
De maildienst op de interne markt aanbieden aan de burgers via een privé- of bedrijfsadres		
Over minstens één operationele e-mail Gateway beschikken om het mailverkeer bij de gebruikers af te leveren		
Een beschrijiving geven van de bestaande platforms (uitrusting en interconnectie) en van de bestaande statische/reactieve en dynamische/proactieve fraudebestrijdingstools (zie paragraaf 3.2) om phishing via e-mail te bestrijden		
Ervoor openstaan om te investeren in een nieuw platform voor het opsporen van frauduleuze e-mails of in de uitbreiding door nieuwe functionaliteiten van hun huidige platform toe te voegen om de opsporing ervan te verbeteren		
Heeft de kandidaat de verschillende oplossingen al geanalyseerd en een mogelijke oplossing getest, bijvoorbeeld via een grootschalig pilotproject?		
De aanvrager moet aantonen dat hij alle geldende wetgeving naleeft, met name op het gebied van de privacybescherming		
De aanvrager moet een realistisch voorstel indienen voor het verzamelen van statistische gegevens om de doeltreffendheid van de oplossing te meten		

2. Technische en operationele vereisten: 60 punten

Criteria	Ja/ Nee	Bewijs
Real-time platform		
Automatic detection		
Language independant		
Behavioral based approach		
Heuristics based behavioral analysis		
Machine Learning		
Computer Vision		
Analyse van het adres van de afzender		
Analyse van het IP-adres		
Analyse van de inhoud van de e-mail		
Analyse van de bijlagen (pdf- en word-bestand, archiefbestand)		
Analyse van de URL('s)		
Analyse van de afbeeldingen (QR-code, afbeelding gebaseerd op tekst en logo)		

Analyse van de metagegevens		
Gebruik van een algoritme voor de opsporing van frauduleuze berichten		
Gedetailleerde beschrijving van de beslissingsmatrix		
Mogelijkheid tot handmatige interventie		

3. Financiële aspecten: 20 punten

Criteria	**Ja/ Nee**	**Bewijs**
Gedetailleerde presentatie van alle uitgesplitste en in detail aangetoonde kosten, d.w.z. een beschrijving van de totale kostprijs voor de oprichting van het platform en de uitsplitsing over de verschillende jaren 2023-2024-2025-2026 voor elke soort uitgave		

4. Projectplan: 10 punten

Criteria	**Ja/ Nee**	**Bewijs**
Gedetailleerd projectplan (met alle fasen) om het fraudebestrijdingssysteem volledig operationeel te maken		

5. Doelstellingen - verwachte resultaten (Informatie en statistische verslagen): 10 punten

Criteria	**Ja/ Nee**	**Bewijs**
Verslag 1: Het aantal e-mails dat in een bepaalde periode werd geblokkeerd ten opzichte van het totale aantal e-mails 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		

6. Andere vereiste informatie.

Criteria	**Ja/ Nee**	**Bewijs**
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.		