CENTRE FOR
CYBERSECURITY
BELGIUM

ACTIVE CYBERBESCHERMING (ACP)

Beleidsdocument, juni 2024

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Inhoudsopgave

Figuren- en tabellenlijst

1. Visie voor de toekomst

De wereld staat nog maar aan het begin van de digitale transitie. Om optimaal te kunnen genieten van de kansen die deze transitie onze samenleving en economie zal bieden, is het cruciaal dat onze burgers, bedrijven en overheden vertrouwen kunnen behouden in het digitale domein. Om dat vertrouwen te garanderen, is cyberveiligheid van cruciaal belang.

De afgelopen jaren is er nationaal en internationaal veel werk verricht om de cyberveiligheid van organisaties en potentiële slachtoffers te verbeteren. Hoewel deze inspanningen cruciaal zijn voor het versterken van de veerkracht van een land, geven recente trends aan dat dergelijke inspanningen onvoldoende kunnen zijn aangezien cyberveiligheidsincidenten, cybercriminaliteit en online fraude blijven toenemen. Volgens het Centrum voor Cybersecurity België (CCB) zijn kwetsbaarheden de oorzaak: zowel menselijke als technische kwetsbaarheden. Als nationale autoriteit voor cyberveiligheid zien wij het als onze taak om organisaties en burgers te helpen deze kwetsbaarheden te overwinnen.

In de loop van de afgelopen jaren heeft het CCB daarom verschillende projecten ontwikkeld om deze kwetsbaarheden aan te pakken via een meer proactieve benadering, die we groeperen onder **het oorspronkelijke concept van Actieve Cyberveiligheid, later omgedoopt tot Actieve Cyberbescherming (ACP staat voor "Active Cyber Protection" in het Engels)**. Een belangrijke beleidsstap werd gezet toen de NIS2-richtlijn het belang van een proactieve aanpak erkende en ACP als wettelijke vereiste opnam in de definitie van nationale cyberveiligheidsstrategieën. Bijgevolg is het nu noodzakelijk voor de EU-lidstaten om in hun nationale cyberveiligheidsstrategieën beleid op te nemen dat ACP implementeert als onderdeel van een alomvattende preventie- en veerkrachtstrategie. Deze ontwikkeling onderstreept het belang van proactieve maatregelen voor de beveiliging van cyberinfrastructuur en waarborgt de veiligheid van digitale communicatie in de hele EU.

Het CCB is sterk overtuigd van de mogelijkheid om actieve cyberbescherming te promoten en wil niet alleen EU-lidstaten, maar ook andere landen aanmoedigen om het ACP-beleid over te nemen. In deze gids willen we ons begrip van het ACP-concept schetsen en enkele van onze ervaringen delen, als die voor anderen van nut kunnen zijn en als ze samenwerking kunnen bevorderen.

Cyberveiligheid is geen project, het is een traject.

Directeur-generaal van het Centrum voor Cybersecurity België,
Miguel De Bruycker, juni 2024

2. Inleiding

In overweging 57 en artikel 7 van Richtlijn 2022/2555 betreffende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de hele Unie, de zogenaamde NIS 2 wet, wordt voor het eerst juridisch verwezen naar het concept van actieve cyberbescherming ("Active Cyber Protection").

De richtlijn bepaalt dat "*de lidstaten, als onderdeel van hun nationale strategieën voor cyberveiligheid, beleid moeten vaststellen ter bevordering van actieve cyberbescherming als onderdeel van een bredere defensieve strategie*."[1] De vorige richtlijn inzake netwerk- en informatiebeveiliging verplichtte de lidstaten al om nationale strategieën voor cyberveiligheid vast te stellen, waarin strategische doelstellingen en prioriteiten worden beschreven. **Actieve cyberbescherming belooft nu een belangrijk aandachtspunt te worden voor nationale autoriteiten en beleidsmakers die nationale cyberveiligheidsstrategieën moeten herzien, bijwerken en aannemen** als onderdeel van hun verplichtingen met betrekking tot de tenuitvoerlegging van NIS2.

Aangezien de EU-lidstaten echter nog steeds bezig zijn met het omzetten van de NIS 2 in nationale wetgeving, is er nog geen gemeenschappelijk begrip, of beter nog, geen gemeenschappelijke definitie, van wat ACP precies betekent en hoe ACP-beleid op nationaal niveau kan worden omgezet. **In dit beleidsdocument wil het CCB zijn interpretatie van het concept schetsen en beste praktijken voor de implementatie ervan delen**.

Overweging 57 van de NIS 2 omschrijft ACP als:

> ***"In plaats van reactief te reageren, is actieve cyberbescherming het voorkomen, detecteren, monitoren, analyseren en beperken van inbreuken op de netwerkbeveiliging op een actieve manier, gecombineerd met het gebruik van capaciteiten die binnen en buiten het slachtoffernetwerk worden ingezet. Dit kan inhouden dat lidstaten gratis diensten of instrumenten aanbieden aan bepaalde entiteiten, zoals zelfbedieningscontroles, detectie-instrumenten en takedown-diensten. Het vermogen om snel en automatisch bedreigingsinformatie en -analyses, waarschuwingen voor cyberactiviteiten en responsmaatregelen te delen en te begrijpen, is van cruciaal belang om een eenheid van inspanning mogelijk te maken bij het succesvol voorkomen, detecteren, aanpakken en blokkeren van aanvallen op netwerk- en informatiesystemen. Actieve cyberbescherming is gebaseerd op een defensieve strategie die offensieve maatregelen uitsluit."***

Het CCB, de nationale autoriteit voor cyberveiligheid in België en verantwoordelijk voor de coördinatie van Europese verplichtingen en vertegenwoordiging, beschouwt ACP als

[1] Zoals vermeld in overweging 57 van Richtlijn (EU) 2022/2555 betreffende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.

een proactieve, op maat gemaakte, geautomatiseerde en participatieve benadering van cyberveiligheid.

Tabel 1 Kenmerken van de CCB-benadering van ACP

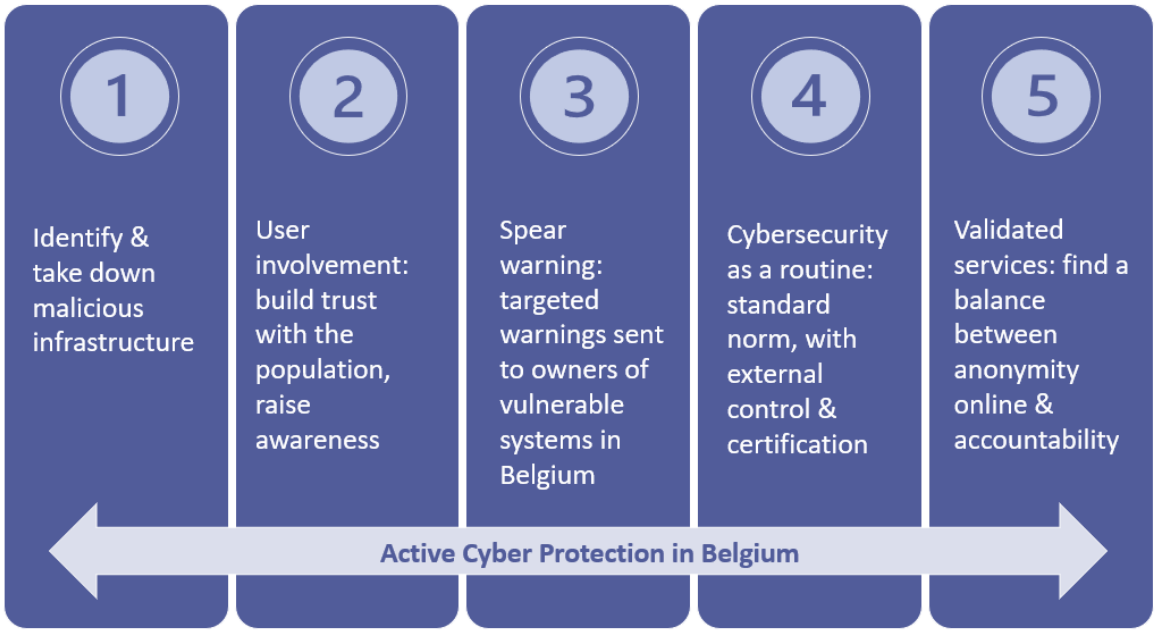
Proactief	In plaats van enkel maar te reageren op aanvallen, zoekt ACP proactief naar potentiële bedreigingen, kwetsbaarheden en kwetsbare systemen, voordat deze op grote schaal kunnen worden uitgebuit. Op die manier ondersteunt ACP de preventie van grote inbreuken op de cyberveiligheid in organisaties.
Op maat	Omdat er geen "*one size fits all*"-oplossing bestaat, promoot ACP oplossingen op maat, rekening houdend met de verschillende behoeften en cyberhouding van belanghebbenden, van individuen en kleine organisaties tot grote bedrijven en overheidsinstellingen, aangepast aan hun sector en systeemconfiguratie. In plaats van waarschuwingen uit te zenden, moedigt ACP het delen van informatie of het aanbieden van diensten per belanghebbende aan, alleen van wat voor hen relevant is, om informatieoverbelasting te voorkomen.
Geautomatiseerd	In een snel veranderend cyberveiligheidslandschap is snelheid essentieel. Er moeten geautomatiseerde oplossingen, bij voorkeur op schaal, worden ontwikkeld om systemen te beschermen tegen steeds meer geautomatiseerde aanvallen. Dergelijke automatisering en schaalbaarheid in de bescherming kunnen ook helpen om het toenemende tekort aan vaardigheden op het gebied van cyberveiligheid op te lossen.
Participatief	ACP moedigt een actieve betrokkenheid aan van alle actoren, van individuen tot grote organisaties, bij het identificeren en verhelpen van kwetsbaarheden op een manier die ten goede komt aan hun organisatie en indien mogelijk aan de bredere samenleving. In plaats van dat er slechts één zwakke schakel nodig is om een aanval mogelijk te maken, wil ACP deze logica omdraaien: er is slechts één waakzame burger nodig om een systeem te helpen beschermen. Iedereen kan een rol spelen in de bescherming.

Het CCB benadrukt dan ook het actieve aspect van ACP. Dit betekent dat het als nationaal CSIRT **actief op pad wil gaan om gebruikers te betrekken en te helpen bij het versterken van hun eigen digitale omgeving en het dynamisch versterken van hun vertrouwen in het digitale domein**. Burgers en bedrijven moeten vooral betrokken worden bij hun eigen bescherming, want activering leidt tot betere samenwerking. België wil gebruikers actief in contact brengen met informatie over concrete dreigingen die voor hen relevant zijn. Deze actieve aanpak bouwt voort op - en wil verder gaan dan - een solide basis van het verstrekken van beleid en richtlijnen, het publiceren van waarschuwingen of het opbouwen van expertise en capaciteiten.

3. De huidige projectpijlers van de actieve cyberbescherming in België

Het CCB beschouwt ACP als een betrouwbaar concept om zijn proactieve beschermingsstrategie in te vatten, in lijn met initiatieven die lopen in verschillende EU-lidstaten en hun respectieve cyberagentschappen. **De kernmissie van het CCB is om van België een van de minst cyberkwetsbare landen in Europa te maken**. Om dit doel te bereiken, **ontwikkelt** het CCB **nationale projecten die niet alleen technische kwetsbaarheden zoals kwaadaardige code aanpakken, maar ook menselijke kwetsbaarheden zoals phishing.**

Deze **projecten zijn momenteel gegroepeerd rond vijf operationele pijlers**: identificeren en uitschakelen van kwaadaardige infrastructuur, betrokkenheid van gebruikers, waarschuwen voor gevaarlijke situaties, cyberveiligheid als een routine en gevalideerde diensten.



Afbeelding 1 De huidige ACP-projectpijlers van het CCB

Alvorens deze pijlers meer in detail te bespreken, is het belangrijk te verduidelijken dat de **CCB-benadering van ACP geen statische onderneming met een eindig doel wil zijn; in plaats daarvan is het een vloeiende en progressieve inspanning**. Het wordt voortdurend herzien en aangescherpt en wordt eerder gezien als een voortdurende reis dan als een taak met een eindstreep. Het doel voor het CCB is om een algemeen kader te creëren dat de flexibiliteit kan bevorderen die nodig is om zich aan te passen aan nieuwe methoden voor cyberaanvallen. Deze proactieve houding is essentieel om voorop te blijven lopen in het steeds veranderende domein van cyberbedreigingen. De vijf huidige pijlers die hieronder worden beschreven, zullen in de toekomst ongetwijfeld worden aangepast.

Pijler I - Kwaadaardige infrastructuur identificeren en uitschakelen

Infrastructuursegmentatieprojecten houden de systematische identificatie in van infrastructuur die gebruikt wordt door kwaadwillende actoren, met als doel om tijdig te waarschuwen voor dergelijke infrastructuur. Vervolgens worden passende maatregelen geïmplementeerd om deze bedreigingen uit te filteren wanneer dat nodig wordt geacht. Deze infrastructurele "segmentatie"-aanpak is gericht op het begrijpen van de activiteiten van kwaadwillende actoren, wat een meer gerichte beveiliging van onze Belgische infrastructuur mogelijk maakt.

Een van de centrale initiatieven van het CCB onder deze projectpijler is het **Belgian Anti-Phishing Shield** (BAPS), in de respectievelijke bijlage vindt u hierover meer details. BAPS, dat in 2021 werd gelanceerd, waarschuwt voor kwaadaardige websites op het Belgische DNS-niveau en sluit daarmee aan bij de dimensie van "actieve mitigatie" die in NIS 2 wordt beschreven.

Het project is opgezet om kwaadaardige links te identificeren en vervolgens elke Belgische gebruiker - klanten van de grote Belgische Internet Service Providers (ISP's) - weg te leiden van die pagina. Als een website die door een internetgebruiker wordt opgevraagd op een lijst met verdachte links staat (de lijst wordt bijgehouden door het CCB), wordt de gebruiker doorgestuurd naar een waarschuwingspagina. De samenwerking met de Belgische internetproviders en het publiek heeft in 2022 niet minder dan 13 miljoen klikken naar verdachte websites kunnen voorkomen, of ongeveer 25 waarschuwingen aan Belgische internetgebruikers per minuut. In het eerste kwartaal van 2024 resulteerde BAPS in 3.03.984 hits op de landingspagina, wat neerkomt op een dagelijks gemiddelde van 97.838 hits. Via het systeem worden elke dag bijna 98.000 Belgen die op een kwaadaardige link hebben geklikt, toch beschermd tegen het bezoeken van kwaadaardige infrastructuur - waardoor deze ineffectief wordt.

Het project is dus proactief, geautomatiseerd, op maat gemaakt en - zoals Pijler II laat zien - ook participatief.

Pijler II - Gebruikersbetrokkenheid

Projecten gegroepeerd rond de pijler van gebruikersbetrokkenheid richten zich op het opbouwen van vertrouwen bij de Belgische bevolking (d.w.z. media, gebruikers, bedrijven, burgers) en het verspreiden van bewustzijn over cyberveiligheid. Deze projecten worden gebrandmerkt onder de naam "Safeonweb" en richten zich zowel op het publiek (@Home) als op organisaties (@Work).

- **Safeonweb@home** gebruikt een mix van communicatiemiddelen om Belgische burgers snel te informeren en te adviseren over online beveiliging en digitale bedreigingen om de kans dat ze het slachtoffer worden van scammers en cybercriminelen te verkleinen. De website www.safeonweb.be biedt voortdurend toegang tot advies over cyberveiligheid. Dit gebeurt ook via sociale mediakanalen, de pers en onze 500+ partners tijdens onze jaarlijkse bewustmakingscampagne, die alle sectoren vertegenwoordigt - publiek, privé, academisch - en reclame (in eigendom,

verdiend en betaald). Safeonweb@home omvat ook onze jaarlijkse bewustmakingscampagne in oktober. Onze partners (bv. de Cybersecurity Coalition en Febelfin) helpen ons niet alleen bij het verspreiden van de boodschap, maar ook bij het ontwikkelen van de inhoud van de campagne. Dankzij hun expertise op het terrein kunnen we de boodschap verfijnen en verduidelijken, zodat ze zoveel mogelijk mensen bereikt die de juiste acties ondernemen om zich te beschermen tegen alle soorten bedreigingen van cyberveiligheid, maar vooral tegen phishing - de echte plaag van onze tijd.

    - Onderdeel van het dienstenpakket van Safeonweb is de Safeonweb mobiele app om internetgebruikers snel op de hoogte te brengen van nieuwe phishing-pogingen en om nieuwe beveiligingstips te versturen (zie bijlage C voor meer details).

- Een recente toevoeging is **Safeonweb@work**. Het doel van dit project is ervoor te zorgen dat ook Belgische bedrijven klaar zijn om te concurreren in een steeds meer gedigitaliseerde wereld. Door hun organisatie en productiemethodes te digitaliseren hebben Belgische bedrijven hun investeringskosten kunnen verlagen, hun processen kunnen optimaliseren en dichter bij hun klanten kunnen komen. Als reactie op deze exponentiële transformatie vergroten steeds meer verbonden en onderling afhankelijke systemen het kwetsbare oppervlak van organisaties en creëren ze nieuwe uitdagingen: het implementeren van cyberveiligheidsmaatregelen om hun activiteiten en investeringen te beschermen. Daarom, en voortbouwend op het succes en de erkenning van Safeonweb.be voor het publiek, lanceerde het CCB in november 2023 een gespecialiseerd platform Safeonweb@work (https://atwork.safeonweb.be/). Via dit platform kunnen Belgische bedrijven en organisaties hun domeinen en IP-bereiken registreren om gebruik te maken van de diensten van Safeonweb@work. Het Safeonweb@work-platform maakt gebruik van het bestaande Early Warning System en biedt een lightversie zodat bedrijven waarschuwingen kunnen ontvangen op basis van de technische informatie die ze hebben geregistreerd. Op dit portaal kunnen organisaties ook maturiteitsbeoordelingen maken en diverse adviesdocumenten, tools, ondersteuning, sjablonen en referenties vinden om hun cyberveiligheidsniveau te verhogen. In bijlage E vindt u meer informatie.

Een van de speerpuntinitiatieven van CCB Safeonweb in de strijd tegen phishing is het **BePhish-project (zie bijlage D)**. Het CCB kan al jaren rekenen op de medewerking van het publiek door verdachte berichten te melden. Het CCB heeft het e-mailadres suspicious@safeonweb.be (in vier talen) gecreëerd waarnaar burgers verdachte berichten (e-mails of sms'jes) kunnen doorsturen. Elke dag ontvangen we duizenden verdachte berichten.

De deelname van de bevolking aan de Safeonweb-projecten, met name het BePhish-project, is een echte illustratie van ACP en is daarom rechtstreeks verbonden met het aspect "betrokkenheid" in de NIS 2-richtlijn. In 2021 werden 4.500.000 berichten doorgestuurd naar suspicious@Safeonweb.be. In 2022 steeg dit aantal verder tot 7 miljoen berichten, wat resulteerde in de detectie van meer dan 660 000 verdachte URL's, een gemiddelde van 15 000

geanalyseerde berichten per dag. In 2023 steeg dit cijfer nog verder tot bijna 10 miljoen, of een gemiddelde van 27.000 e-mails per dag. Al deze doorgestuurde links worden vervolgens gebruikt voor andere projecten, zoals BAPS.

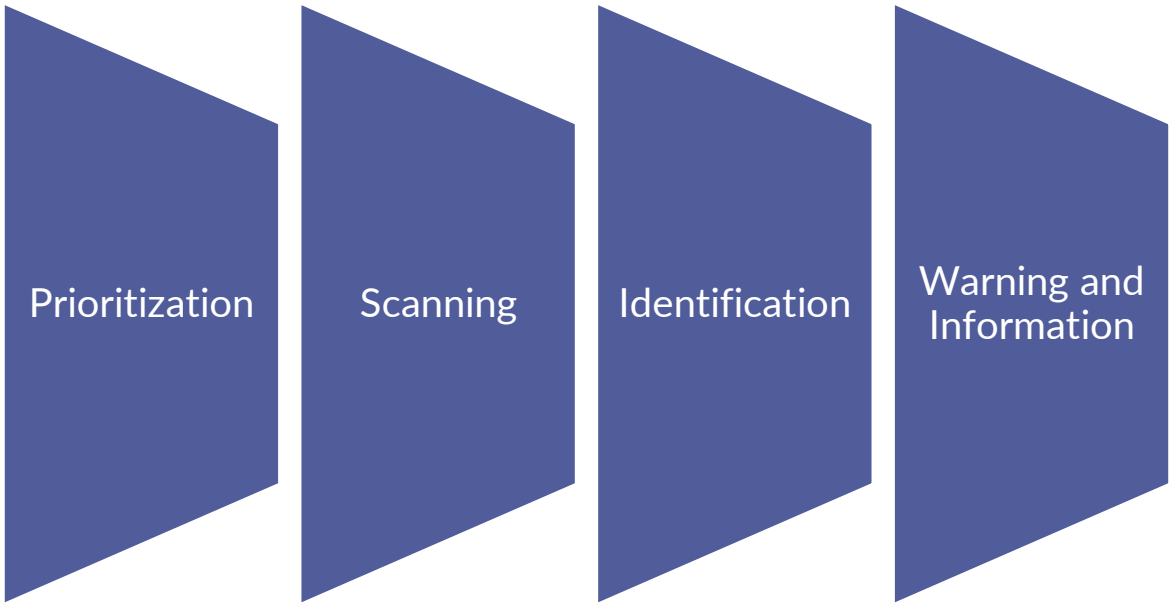
Pijler III – Spear Warning Proces

Terwijl Spear Phishing met succes wordt gebruikt om gerichte berichten naar individuen te sturen om in hun systemen te komen, gebruikt het CCB dezelfde aanpak maar met als doel bescherming te leveren: spear warning.

Een belangrijk onderdeel van ACP is de ***realtime* detectie van bedreigingen**. Tijdige identificatie stelt organisaties in staat om snel te reageren en zo potentiële schade te minimaliseren. Spear Warning-projecten zijn speciaal ontworpen om organisaties te helpen kwetsbare systemen op te sporen.

De CCB verzamelt systematisch informatie over kwetsbare systemen, met inbegrip van bedreigingen, kwetsbaarheden en inbraken, en houdt een lijst bij van de kwetsbare systemen in België waarvan de kans op misbruik het grootst is. Vervolgens gaat het CCB proactief op zoek naar de eigenaars van deze kwetsbare systemen. Na identificatie geeft het CCB een individuele en op maat gemaakte waarschuwing af aan de eigenaar van het kwetsbare systeem, waarbij gebruik wordt gemaakt van geautomatiseerde processen voor een snelle en directe aanpassing. **Deze aanpak draagt actief bij aan het verkleinen van het aanvalsoppervlak van een organisatie, waardoor het voor potentiële aanvallers moeilijker wordt om zwakke plekken in het systeem uit te buiten.** Het CCB heeft herhaaldelijk gemerkt hoe gerichte waarschuwingen de mate waarin kwetsbare organisaties actie ondernemen aanzienlijk verhogen.

Een bekend initiatief onder deze pijler is het **Early Warning System (EWS, zie bijlage B).** Dit initiatief is op maat gemaakt om waarschuwingen te geven aan organisaties van vitaal belang (zoals netwerk- en informatiebeveiliging, kritieke infrastructuren, nucleaire operatoren en de gegevensbeschermingsautoriteit) en organisaties van bijzonder belang op nationaal niveau in België. De implementatie van EWS sluit naadloos aan bij het concept van "actieve mitigatie" zoals uiteengezet in de NIS2 Richtlijn.



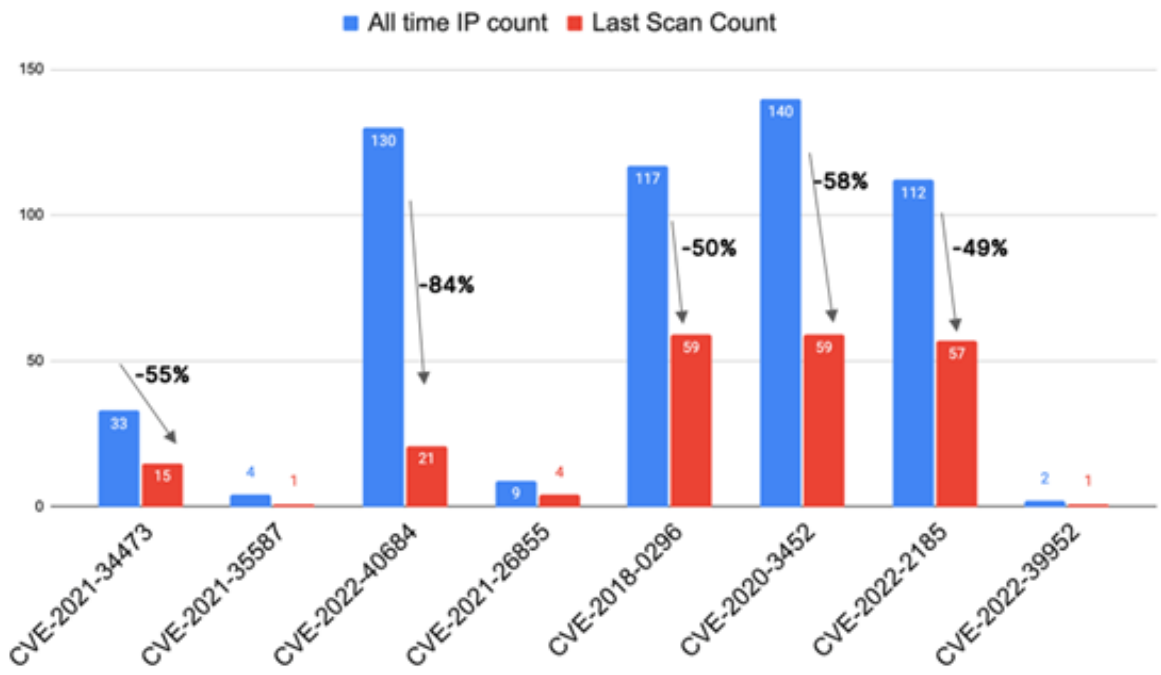
Figuur 2 de vier verschillende fasen van EWS

Het waarschuwingsproces van EWS verloopt in vier verschillende fasen: prioriteitsbepaling; scanning; identificatie; waarschuwing en informatie. In detail:

- **Prioriteitsbepaling:** samen met Recorded Future, onze commerciële partner, evalueren we de kwetsbaarheden waarvan de kans het grootst is dat ze worden uitgebuit.
- **Scannen:** vervolgens voert het CCB een grondige scan uit van de Belgische IP-ruimte om de belangrijkste kwetsbare systemen voor de geprioriteerde kwetsbaarheden te identificeren. Hiervoor hebben we een wettelijk mandaat. Aangezien landen geen exacte IP-grenzen hebben, kunnen we alleen die IP-bereiken scannen waarvan met grote zekerheid kan worden aangenomen dat ze in België liggen. Wat beschouwd kan worden als "de Belgische IP-ruimte" is natuurlijk vaag, maar het deel van de systemen dat hierdoor niet gescand kan worden is triviaal.
- **Identificatie:** de volgende stap is het identificeren van de eigenaars van de kwetsbare systemen. Meestal moet de lijst met IP-adressen en tijdsstempel per ISP worden opgesplitst en moeten we de contactinformatie van de eigenaren opvragen bij de ISP's.
- **Waarschuwen en informeren:** als laatste stap worden gerichte waarschuwingen verstuurd naar de eigenaren van kwetsbare systemen. Dit wordt vergemakkelijkt door geautomatiseerde processen voor snelle communicatie. E-mails worden meestal verstuurd naar de IT-beheerder van het kwetsbare systeem.

Het CCB heeft gemerkt welke impact een directe, gerichte en op maat gemaakte melding heeft wanneer deze wordt geschreven door de nationale autoriteit voor cyberveiligheid in vergelijking met een generieke waarschuwing voor een kwetsbaarheid. Toch passen nog steeds niet alle gewaarschuwde eigenaren de noodzakelijke en dringende software-updates onmiddellijk toe. Vaak blijven actief misbruikte kwetsbaarheden te lang

ongepatchet door een gebrek aan urgentie op het niveau van de IT-manager. Daarom stuurt het CCB ook brieven op papier, ondertekend door de directeur-generaal van het CCB, naar de CEO, of een andere wettelijke vertegenwoordiger, van de organisatie.



Afbeelding 2 Verminderingspercentage na speerpuntwaarschuwingsproces

Tijdens het eerste kwartaal van 2024 werden 5757 spear warnings verstuurd naar Belgische organisaties en personen. Omdat het cyberdreigingslandschap altijd in beweging is, begon het CCB naast waarschuwingen voor kwetsbaarheden ook waarschuwingen te versturen voor gelekte referenties en voor malware-infecties die tot aanzienlijke schade zouden kunnen leiden. Dit soort infecties leidt vaak tot ransomware-aanvallen. Daarom kan worden aangenomen dat CCB dankzij deze campagne een aantal ransomware-incidenten heeft kunnen voorkomen, hoewel we nooit zullen weten hoeveel precies.

Gezien deze cijfers en acties is het geen verrassing dat het Spear Warning Project in 2023 de eerste plaats van de Publica Awards in de categorie "beveiliging & veiligheid" in de wacht sleepte.

Pijler IV - Cyberveiligheid als routine

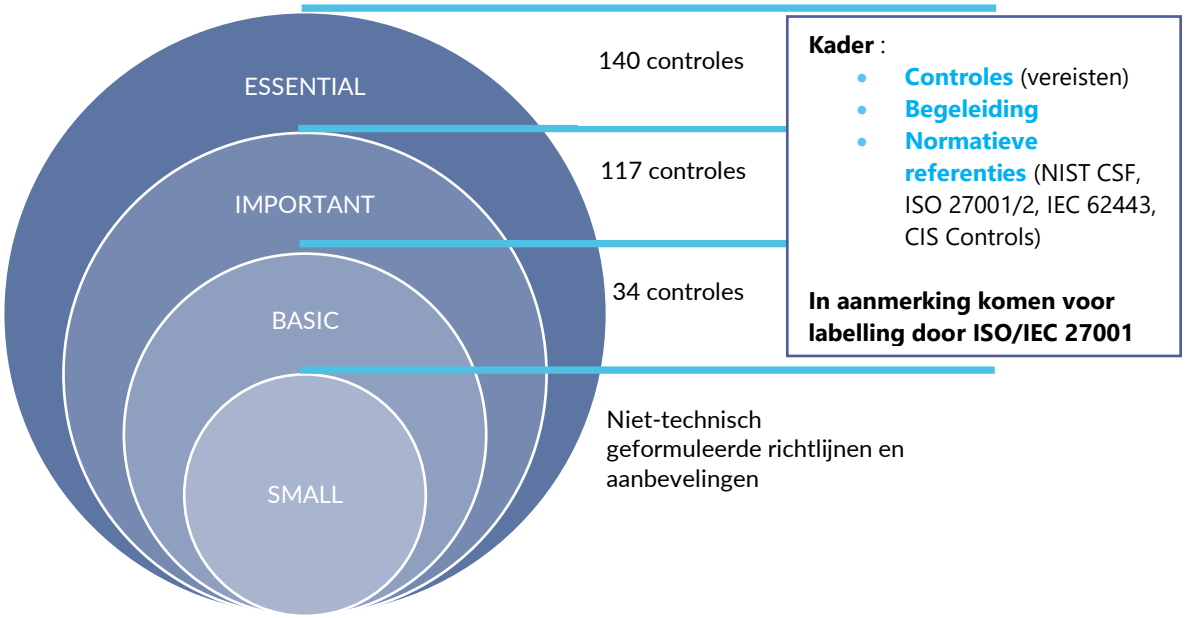
Net zoals brandveiligheid of inbraakbeveiliging deel uitmaakt van de beveiligingsroutine van een organisatie, **is het CCB van mening dat cyberveiligheidsnormen en -standaarden ook deel zouden moeten uitmaken van de beveiligingsroutine van elke organisatie**. Voor organisaties die al onder strikte wettelijke cyberveiligheidseisen vallen, kan het implementeren van actieve cyberveiligheidsmaatregelen helpen om aan hun nalevingsnormen te voldoen. Voor organisaties waar cyberveiligheidseisen niet verplicht zijn, zal het opbouwen van een

routine met standaardnormen, controles, keurmerken en certificeringen hen helpen hun niveau van cyberveiligheid te verhogen.

Het CCB heeft daarom de CyberFundamentals ontwikkeld, gebaseerd op vier fundamentele kaders, om standaardbeveiligingsnormen, externe controles en certificeringen in te voeren voor alle belanghebbenden op alle niveaus. Om internationaal gebruik te vergemakkelijken, zijn er geen specifieke verwijzingen opgenomen met betrekking tot nationale wetgeving. Het model bestaat uit vier niveaus: small, basis, belangrijk en essentieel, en is qua aantal controles op een samenhangende manier opgebouwd. Bovendien zijn **de CyberFundamentals opgebouwd rond vijf kernfuncties**: identificeren, beschermen, detecteren, reageren en herstellen.

- **Identificeren:** deze functie helpt bij het ontwikkelen van een organisatorisch begrip van hoe cyberveiligheidsrisico's met betrekking tot systemen, mensen, bedrijfsmiddelen, gegevens en capaciteiten moeten worden beheerd.
- **Beschermen:** deze functie richt zich op het ontwikkelen en implementeren van de beveiligingen die nodig zijn om een cyberrisico te beperken of in te perken.
- **Detecteren:** het doel van deze functie is te zorgen voor de tijdige detectie van cyberveiligheidsgebeurtenissen.
- **Reageren:** deze functie draait om de controles die helpen reageren op cyberveiligheidsincidenten. De respond-functie ondersteunt het vermogen om de impact van een potentieel cyberveiligheidsincident in te dammen.
- **Herstellen:** deze functie richt zich op de beveiligingen die helpen de veerkracht te behouden en diensten te herstellen die zijn getroffen door een cyberveiligheidsincident.

Met de CyberFundamentals kan cyberveiligheid een routine worden. Er is een aanvullende toolbox gemaakt om organisaties te begeleiden bij de implementatie van het raamwerk. De CyberFundamentals is gebaseerd op het Cybersecurity Framework van het National Institute of Standards and Technology (NIST/CSF) en aangevuld met relevante inzichten uit andere normen, waaronder ISO 27001/ISO 27002 (voor het opzetten van een beheersysteem voor informatiebeveiliging), IEC 62443 (cyberveiligheid voor operationele technologie in automatiserings- en besturingssystemen.) en de CIS Critical Security Controls (ETSI TR 103 305-1). Het schema is gevalideerd door het Federal Cyber Emergency Response Team (CERT.be), dat de (geanonimiseerde) informatie over cyberaanvallen in de echte wereld heeft verstrekt. Deze gegevens werden gebruikt om de aanvalsdekkingspercentages te verkrijgen. De CyberFundamentals zullen voortdurend worden bijgewerkt en verbeterd, rekening houdend met de feedback van belanghebbenden, het evoluerende risico van specifieke cyberveiligheidsbedreigingen, de beschikbaarheid van technische oplossingen en voortschrijdend inzicht.



Afbeelding 3 Overzicht van het CyberFundamentals Framework

Op basis van historische gegevens van het CCB is nadien een analyse gemaakt van succesvolle cyberaanvallen met behulp van geanonimiseerde gegevens. De conclusie is dat; maatregelen op zekerheidsniveau basis 82% van de aanvallen konden afdekken; maatregelen op zekerheidsniveau belangrijk 94% van de aanvallen konden afdekken; maatregelen op zekerheidsniveau essentieel 100% van de aanvallen konden afdekken. Op basis van deze aanvallen werden op elk niveau belangrijke maatregelen geïdentificeerd om prioriteit te geven aan de tegenmaatregelen ter bescherming tegen de bekende cyberaanvallen die relevant zijn voor dat zekerheidsniveau. Zie Bijlage F voor meer informatie.

Pijler V - Gevalideerde diensten

Het internet biedt gebruikers anonimiteit. Het concept van anonimiteit is echter een tweesnijdend zwaard. Hoewel het een gevoel van bevrijding kan bevorderen, kan het ook kwaadaardige activiteiten stimuleren. Zonder verantwoording kunnen individuen de anonimiteit misbruiken voor schadelijke activiteiten. Dit leidde tot een groeiende behoefte aan validatie om deze negatieve aspecten tegen te gaan. Terwijl fraudepreventietechnologie steeds geavanceerder wordt, houden tactieken voor accountovername gelijke tred. Volgens onderzoekers nemen accountovername-aanvallen nog steeds toe en vormen ze een probleem als het geldelijke verliezen betreft en het niet te kwantificeren verlies van geloofwaardigheid en vertrouwen van klanten.

Bovendien lijken recente technologieën, zoals generatieve AI, eerdere technieken zoals slimme social engineering, phishing en andere soorten aanvallen aan te wakkeren, waardoor hackers een ongeëvenaarde toegang krijgen tot persoonlijk identificeerbare informatie, waardoor ze een accountovername door consumenten kunnen starten. Daardoor wordt authenticiteit steeds complexer om aan te tonen.

Het is dit specifieke raadsel - hoe ervoor te zorgen dat wat online verschijnt veilig en gevalideerd is - dat ertoe leidde dat het CCB zich begon af te vragen hoe ervoor kan worden

gezorgd dat online aanwezigheid kan worden beveiligd. Vanwege de toename van het aantal frauduleuze websites die gebruikt worden voor phishing, d.w.z. om persoonlijke gegevens van gebruikers te verkrijgen voor illegale doeleinden, creëerde het CCB de **pijler Gevalideerde diensten van ACP.**

Een van de fundamentele aspecten van een veilige online omgeving is het zoeken naar een evenwicht tussen anonimiteit en validatie. Het is belangrijk dat **de vrijheid die anonimiteit biedt, niet in strijd is met de toenemende behoefte aan online validatie voor veiligheidsdoeleinden**. Het is even belangrijk om aansprakelijkheids- en verantwoordingslagen in te voeren om gevalideerde diensten aan te bieden. Validatiemechanismen moeten worden geïmplementeerd waar persoonlijke/gevoelige/kritieke informatie wordt gebruikt, om zowel privacy- als veiligheidsredenen. Digitale identiteiten gekoppeld aan echte referenties kunnen kwaadwillende afschrikken en een omgeving van vertrouwen en geloofwaardigheid creëren.

Met het project "gevalideerde sites" heeft het CCB een **browserplugin** ontwikkeld om het betrouwbaarheidsniveau van websites (sterke uitgevervalidatie, geen uitgevervalidatie eigenaar, of bekende kwaadaardige website) te beoordelen en aan te geven aan gebruikers. Deze plugin zal beschikbaar zijn op laptops en desktopcomputers met als doel 90% groen licht ervaring in België bij het online surfen (zie bijlage G voor meer details). De projecten voor gevalideerde diensten houden rechtstreeks verband met de dimensie "vertrouwen" die wordt gebruikt om ACP te definiëren in NIS 2. Tegelijkertijd is het project voor gevalideerde sites in overeenstemming met de EUid-verordening, die de vorige eIDAS-verordening herziet. Met deze Verordening wil de EU diensten voor websiteauthenticatie bevorderen als een manier om het vertrouwen in online diensten te vergroten, door gebruikers de zekerheid te bieden dat er een echte en legitieme entiteit achter de website staat die ze bezoeken.

4. Conclusies en verdere stappen

Cyberveiligheid is geen project, het is een traject. Het is een doorlopend proces dat voortdurende aanpassing en samenwerking vereist. In de onderling verbonden wereld van vandaag ontwikkelen cyberbedreigingen zich voortdurend, waardoor een dynamische en proactieve aanpak nodig is. Organisaties en individuen moeten cyberveiligheid niet zien als een eenmalige inspanning met een vastgesteld eindpunt, maar eerder als een voortdurende expeditie naar veerkracht en paraatheid. Dit beleidsdocument geeft inzicht in het strategische kader dat is aangenomen door het CCB. In dit verband wordt het belang benadrukt van **proactieve, op maat gemaakte, geautomatiseerde en participatieve projecten langs vijf actuele pijlers.**

Bijgevolg **erkent** het **CCB de belangrijke rol van nationale cyberveiligheidsinstanties die proactieve maatregelen nemen en gebruikers ondersteunen bij het identificeren en verhelpen van zwakke plekken voordat ze bezwijken onder cyberdreigingen**. Het **CCB** erkent de wettelijke verplichtingen die zijn vastgelegd in de NIS 2-richtlijn en de uitgebreide definitie van ACP, maar erkent **dat dit streven niet geïsoleerd kan worden nagestreefd**. Autoriteiten moeten samenwerken, niet alleen met de private sector, maar ook met elkaar. Daarom onderstreept het CCB het belang van het overwegen van de internationale dimensie van ACP-initiatieven, het erkennen van hun rol in het bevorderen van internationale betrekkingen en samenwerking binnen het cyberdomein, en de mogelijkheden om ACP-projecten te versterken.

In het licht van dit perspectief **nodigt** het **CCB internationale partners uit, zowel uit de publieke als de private sector, om deel te nemen aan de inspanningen en gezamenlijk te brainstormen over innovatieve strategieën**. Het CCB moedigt alle geïnteresseerde partijen aan om contact op te nemen en interesse te tonen in samenwerking of het delen van informatie over de principes die in dit document zijn verwoord.

Geïnteresseerde partijen worden nu al aangemoedigd om de bijlagen bij dit document te bestuderen, waar gedetailleerde informatie wordt verstrekt over specifieke CCB-projecten die integraal deel uitmaken van het ACP-kader. Deze bijlage dient als een beknopte opslagplaats voor beste praktijken en biedt mogelijkheden voor potentiële samenwerking. Door deze details door te nemen, kunnen geïnteresseerde belanghebbenden inzicht krijgen in lopende initiatieven van de CCB, wat de uitwisseling van expertise en middelen vergemakkelijkt. De bijlage wordt zo een vitale bron voor degenen die hun betrokkenheid bij het ACP-kader, zoals vertaald door de CCB, willen verdiepen en willen bijdragen aan de doelstellingen van de CCB om de veerkracht van cyberspace op nationaal en internationaal niveau te vergroten.

Door een omgeving van samenwerking en gedeelde expertise aan te moedigen, wil **België zijn cyberweerbaarheid versterken en bijdragen aan de wereldwijde inspanningen om cyberbedreigingen te bestrijden**.

Bijlage

HET BELGISCHE ANTI PHISHING SHIELD (BAPS)	
Webpagina	WAARSCHUWING (BAPS) (Safeonweb.be)
Doel	De klikfrequentie van kwaadaardige websites in de Belgische cyberspace verlagen.
Project	Het Belgian Anti Phishing Shield (BAPS) werd in 2021 gelanceerd om internetgebruikers te waarschuwen voor kwaadaardige websites op Belgisch DNS-niveau. Als de door een internetgebruiker opgevraagde website op een lijst met verdachte links staat - die door het CCB wordt bijgehouden - wordt de gebruiker doorgestuurd naar een waarschuwingspagina.
Hoe het werkt	BAPS is gebouwd op het BePhish-project (zie hieronder). Verdachte weblinks worden naar het CCB gestuurd via het e-mailadres suspicious@safeonweb.be. Het is ook mogelijk om een screenshot van een frauduleuze sms en QR-code te sturen. Onze technologie is in staat om URL's in afbeeldingen en QR-codes te detecteren. Domeinen worden gecontroleerd op inhoud en komen op de zogenaamde "BAPS-lijst" met kwaadaardige websites terecht als er geen inhoud kan worden gevonden. Verdachte URL's worden doorgestuurd naar Google Safe Browsing en Microsoft SmartScreen. De browsers gebruiken deze informatie om internetgebruikers te waarschuwen voor schadelijke websites. Aangezien het CCB geen controle heeft over de snelheid waarmee Google en Microsoft reageren op deze lijst van kwaadaardige links, hebben het CCB en de Belgische internetproviders Belnet, Proximus, Telenet en Orange een procedure ontwikkeld om internetgebruikers in real time te waarschuwen: telkens wanneer een gebruiker op een link klikt, wordt een DNS-verzoek naar de internetprovider (ISP) gestuurd. Dankzij BAPS vergelijkt de DNS-server van de ISP de opgevraagde website met de lijst van kwaadaardige websites. **Als de opgevraagde website op deze lijst staat, stuurt de DNS-server van de ISP de gebruiker door naar een waarschuwingspagina**. De lijst met schadelijke websites wordt weer gevoed door de doorgestuurde berichten die via het BePhish-project worden ontvangen.
Cijfers	De samenwerking met het Belgische publiek voorkwam niet minder dan 13 miljoen kliks naar verdachte websites in 2022, of ongeveer 25 waarschuwingen aan internetgebruikers per minuut. In het tweede kwartaal van 2023 resulteerde BAPS in 2.064.378 hits op de landingspagina, wat neerkomt op een dagelijks gemiddelde van 33.842 hits.

EARLY WARNING SYSTEM (SYSTEEM VOOR VROEGTIJDIGE WAARSCHUWING)	
Doel	Het aantal kwetsbaarheden en het tijdsbestek van bedreigingen voor Organisaties van Vitaal en Bijzonder Belang in België verminderen.
Projectbeschrijving	Het Early Warning System (EWS) is een online uitzendplatform dat werd gecreëerd om organisaties van vitaal of bijzonder belang in België op een snelle en gestandaardiseerde manier te waarschuwen voor kwetsbaarheden, inbraken en andere cyberdreigingen of -aanvallen die relevant zijn voor hun sector of zelfs hun organisatie. Een speciaal Cyber Threat and Intelligence Sharing-team houdt dagelijks het (dark) web in de gaten op kwetsbaarheden zoals het lekken van credentials. De waarschuwingen zijn gebaseerd op informatie die het CCB ontvangt en filters van een breed scala aan zowel publieke als private partners, nationaal en internationaal. Deze informatie wordt zowel uitgezonden als individueel gericht gedeeld. • Na onboarding kunnen geregistreerde organisaties vrij een archief raadplegen met strategische en operationele rapporten en meldingen die relevant zijn voor hun sector. Op de portal wordt ook dagelijks een algemeen rapport over het dreigingslandschap gepubliceerd. Meldingen van nieuw beschikbare informatie worden via e-mail verzonden naar de aangemelde deelnemers. Dit kan in realtime of in de vorm van een samenvatting. • Op een gerichte manier worden waarschuwingen, indicators of compromise (IoC) en rapporten rechtstreeks naar organisaties van vitaal of speciaal belang gestuurd. Dergelijke waarschuwingen stellen kiezers in staat om snel relevante informatie te verkrijgen uit een betrouwbare bron en zo snel mogelijk te handelen om zichzelf te beschermen tegen actieve bedreigingen.
Wettelijk kader	Een van de moeilijkste onderdelen van het opzetten van een spear warning-dienst op nationaal niveau was het verkrijgen van alle noodzakelijke wettelijke bepalingen. Het kostte het CCB heel wat moeite om de juiste balans te vinden en de politieke autoriteiten te overtuigen. Het CCB heeft nu de wettelijke opdracht om cyberbedreigingen en kwetsbaarheden op te sporen die kunnen leiden tot aanzienlijke cyberaanvallen en schade. Het CCB kan niet-discriminerende en niet-opdringerige scans uitvoeren, waarbij de proportionaliteit wordt gerespecteerd en alleen informatie wordt verzameld die nodig is om de kwetsbaarheid te identificeren, met als enige doel de eigenaar van het kwetsbare systeem onmiddellijk te informeren. Er was nog een wetgevingsinitiatief nodig om het CCB in staat te stellen identiteits- en contactgegevens te verkrijgen. Dankzij dit nieuwe wettelijke kader en een constructieve samenwerking met de serviceproviders kunnen we de meeste bedrijven die risico lopen binnen een paar dagen na het ontdekken van de kwetsbaarheid identificeren en op de hoogte stellen.
Cijfers	Het CCB heeft in de eerste drie kwartalen van 2023 8000 waarschuwingen verstuurd. Afhankelijk van de kwetsbaarheid kunnen we een snelle afname meten variërend van 50% tot 90% binnen enkele dagen, in plaats van weken

	of maanden. Het effect is aanzienlijk, zelfs voor oudere kwetsbaarheden waarvoor al meerdere algemene waarschuwingen zijn gepubliceerd. Naast de waarschuwingen voor kwetsbaarheden is het CCB ook begonnen met het versturen van waarschuwingen voor gelekte referenties en voor malware-infecties die tot aanzienlijke schade kunnen leiden.

SAFEONWEB@HOME: SAFEONWEB-APP	
Webpagina	Safeonweb app | Safeonweb
Doel	De belangrijkste menselijke eigenschappen waar cybercriminelen misbruik van maken zijn onwetendheid en goedgelovigheid. Met dit project wil het CCB de algemene bevolking bewuster maken van phishing en online oplichting door te laten zien dat niet elk bericht te vertrouwen is en dat je nooit helemaal zeker weet wie een bericht heeft verstuurd. Regelmatig en effectief waarschuwen voor directe bedreigingen kan een groot verschil maken zonder angst en overdreven wantrouwen te willen creëren.
Project	De Safeonweb-app is een mobiele applicatie voor Android en iOS mobiele apparaten. De app stuurt waarschuwingen over actuele cyberdreigingen in België op een vergelijkbare manier als nieuwsflits-apps. De Safeonweb-app is gratis beschikbaar voor iOS (App Store) en Android (Google Play Store).

BEPHISH	
Webpagina	Wat is suspicious@Safeonweb.be? | Safeonweb
Doel	Burgers worden aangemoedigd om niet alleen op te letten op verdachte e-mails via onze app, maar ook om actie te ondernemen. Ze kunnen verdachte e-mails of sms-berichten doorsturen naar het CCB e-mailadres suspicious@safeonweb.be. Door de bevolking te activeren, blijft hun aandacht voor phishingberichten langer en meer betrokken. Het doel van BePhish is om het bewustzijn over de nieuwste phishingcampagnes verder te vergroten en de slagingskans van phishing zoveel mogelijk te verminderen en tegen te gaan.
Project	Het CCB roept internetgebruikers op om verdachte berichten door te sturen naar het e-mailadres suspicious@safeonweb.be (beschikbaar in het Nederlands, Frans, Duits en Engels). Uit de ontvangen verdachte berichten en URL's haalt het CCB bijlagen en links. Vervolgens worden bijlagen automatisch geanalyseerd. In het geval van bijlagen wordt een sandbox gebruikt. Als uit de analyse blijkt dat een URL kwaadaardig is, wordt deze doorgestuurd naar Google Safe Browsing en Microsoft Smartscreen. Deze twee lijsten met schadelijke websites worden door de meeste browsers gebruikt om een waarschuwing op browserniveau te geven. Op deze manier worden internetgebruikers gewaarschuwd als ze op een schadelijke link hebben geklikt. Verdachte links "voeden" ook het BAPS-project. Ze worden doorgestuurd naar Google en Microsoft Safe Browsing, waardoor de grote browsers internetgebruikers kunnen waarschuwen. Op deze manier worden ook minder oplettende internetgebruikers die op de link klikken beschermd.
Cijfers	In 2021 werden 4.500.000 berichten doorgestuurd naar suspicious@safeonweb.be. In 2022 steeg dit aantal verder tot 7 miljoen berichten, wat resulteerde in de detectie van meer dan 660.000 verdachte

	URL's. In 2023 ontving het CCB bijna 10.000.000 berichten van de bevolking, een gemiddelde van 27.000 e-mails per dag. Dit resulteerde in de detectie van bijna 1,3 miljoen verdachte URL's.

SAFEONWEB@WORK	
Webpagina	Safeonweb@work - homepage | CCB Safeonweb
Doel	Het Safeonweb@work-project heeft als doel het niveau van cyberveiligheid van Belgische bedrijven en organisaties te verhogen door hen te voorzien van inhoud, tools en diensten zoals kwetsbaarheidsdetectie, waarschuwingen, templates, advies en ondersteuning.
Project	Het Safeonweb@work-platform bestaat uit 2 delen: een website en een portaal met beveiligde aanmelding. • De website is publiek beschikbaar en verzamelt tools en diensten voor Belgische bedrijven en organisaties om hun maturiteit te evalueren en verschillende adviesdocumenten, tools, ondersteuning, aanpasbare beleidssjablonen om het beheer van informatiebeveiliging op te starten, zelfevaluaties om lacunes in cyberveiligheid te identificeren en referenties om hen te helpen hun niveau van cyberveiligheid te verhogen, zowel op korte als op lange termijn. • Het portaal heeft een authenticatiemechanisme op basis van eID (in België "ItsMe" genoemd) en vertrouwt op de Federale Authenticatiedienst (FAS). Eenmaal geauthentiseerd in het portaal, kunnen Belgische bedrijven en organisaties hun contactgegevens en netwerkinformatie (domeinnamen, IP-adressen, IP-bereiken) invullen. Het portaal gebruikt een lightversie van het bestaande Early Warning System om waarschuwingen te sturen naar geregistreerde bedrijven op basis van de geregistreerde technische informatie. Na voltooiing en registratie kunnen gebruikers speciale diensten activeren, zoals de Cyber Threat Alerts (waarschuwingen per e-mail ontvangen als er een kwetsbaarheid of infectie wordt gedetecteerd op hun netwerkmiddelen), het Quick Scan Report (een jaarlijkse momentopname van het domein en netwerk van de organisatie waarin bedreigingen worden geïdentificeerd en mitigerende acties worden beschreven).

CYBERFUNDAMENTALS FRAMEWORK (CYFUN)	
Webpagina	CyberOnderzoekskader | CCB Safeonweb
Doel	Het CyberFundamentals Framework heeft als doel de cyberweerbaarheid van een organisatie te vergroten, het risico op de meest voorkomende cyberaanvallen aanzienlijk te verkleinen en gegevens te beschermen, zodat zoveel mogelijk bedrijven voldoen aan de basisprincipes voor cyberveiligheid.
Project	CyFUN is ontwikkeld op basis van internationale normen en kaders op het gebied van ICT en industriële cyberveiligheid. De implementatie van CyFUN kan vertrouwen opbouwen tussen organisaties en biedt ook ondersteuning voor naleving van regelgeving. Het raamwerk is opgebouwd uit vier niveaus en kan door elke organisatie worden gebruikt, ongeacht de omvang, sector of volwassenheid op het gebied van cyberveiligheid. De vier niveaus bouwen zich op in termen van het aantal controles op een samenhangende manier. Met CyFUN kan het cyberveiligheidsvolwassenheidsniveau in de loop van de tijd worden verhoogd, zodat geïnvesteerde middelen kunnen resulteren in een samenhangende verhoging van de cyberveiligheid. • **Assurance level SMALL biedt** een leidraad voor micro-entiteiten of entiteiten die geen ervaring hebben met cyberveiligheid. • **Assurantieniveau BASIC** kan 82% van de aanvallen afdekken, • **Betrouwbaarheidsniveau BELANGRIJK** kan 94 % van de aanvallen afdekken, • **Zekerheidsniveau ESSENTIAL** kan 100% van de aanvallen dekken, gebaseerd op historische gegevens. Het CCB CyberFundamentals Framework is opgebouwd rond vijf kernfuncties: identificeren, beschermen, detecteren, reageren en herstellen. Deze functies maken het mogelijk om, ongeacht de organisatie en branche, de communicatie rondom cyberveiligheid te bevorderen tussen zowel technische vakmensen als belanghebbenden, zodat cyber gerelateerde risico's kunnen worden opgenomen in de algehele risicomanagementstrategie van de organisatie. Certificering of labeling is mogelijk via onpartijdige en competente geaccrediteerde conformiteitsbeoordelingsinstanties (CAB's) die verificatie- (BASIC/IMPORTANT) of certificeringsaudits (ESSENTIAL) uitvoeren. CyFUN kan ook worden gebruikt als hulpmiddel om de naleving van de NIS2-vereisten voor cyberveiligheid aan te tonen.
Hoe het werkt	CyFUN is gebaseerd op het Cybersecurity Framework van het National Institute of Standards and Technology (NIST/CSF) en aangevuld met relevante inzichten uit andere normen, waaronder ISO 27001/ISO 27002 (voor het opzetten van een beheersysteem voor informatiebeveiliging), IEC 62443 (cyberveiligheid voor operationele technologie in automatiserings- en besturingssystemen.), de CIS Critical Security Controls (ETSI TR 103 305-1). Het schema is gevalideerd door het Federal Cyber Emergency Response Team (CERT.be), dat de (geanonimiseerde) informatie over cyberaanvallen in de echte wereld heeft geleverd. Deze gegevens werden gebruikt om de

	aanvalsdekkingspercentages te verkrijgen. • **Met het startniveau Small kan** een organisatie een eerste beoordeling maken. Het is bedoeld voor micro-organisaties of organisaties met beperkte technische kennis. • **AL Basic** (34 beveiligingscontroles) bevat de standaardvereisten voor informatiebeveiliging voor alle ondernemingen. Deze bieden een effectieve beveiligingswaarde met technologie en processen die al beschikbaar zijn. Waar nodig worden de maatregelen aangepast en verfijnd. Voortbouwend op het basisniveau worden beveiligingseisen toegevoegd om organisaties te beschermen tegen verhoogde cyberrisico's om een hoger niveau van zekerheid te bereiken. 82% van de CERT-aanvalprofielen wordt gedekt door vereisten op niveau BASIC. • **AL Belangrijk** (117 beveiligingscontroles) is ontworpen om de risico's van gerichte cyberaanvallen door actoren met gemeenschappelijke vaardigheden en middelen naast bekende cyberveiligheidsrisico's te minimaliseren. 94% van de CERT-aanvalprofielen vallen onder vereisten op niveau BELANGRIJK • **AL Essential** (140 beveiligingscontroles) gaat een stap verder om ook in te spelen op het risico van geavanceerde cyberaanvallen door actoren met uitgebreide vaardigheden en middelen. 100% van de CERT-aanvalprofielen wordt gedekt door vereisten op niveau ESSENTIAL

SAFEONWEB BROWSER EXTENSIE	
Webpagina	Safeonweb Browseruitbreiding
Doel	De Safeonweb Browser Extension is een internetbrowseruitbreiding die het vertrouwen meet dat u kunt hebben in de websites die u bezoekt. Zo kan een bezoeker van die site er zeker van zijn dat het in orde is om persoonlijke gegevens op die site achter te laten. Als een website niet in staat is om zijn eigenaar te bewijzen, kan het nog steeds een betrouwbare website zijn, met niet-malafide inhoud, maar men moet misschien twee keer nadenken voordat men persoonlijke gegevens op die site achterlaat, omdat er geen garantie is wat voor soort organisatie er achter die website zit.
Project	Voor elke website die u bezoekt, laat de Safeonweb Browser Extension zien of de eigenaar is gevalideerd (Groen) of niet (Oranje). Websites zonder een gevalideerde eigenaar (Amber) kunnen alleen worden gelezen. Voor het delen van persoonlijke en gevoelige informatie kunt u verwachten dat de eigenaar van de website is gevalideerd (Groen). Als een hacker schadelijke inhoud plaatst op een website met een gevalideerde eigenaar, verandert de validatiestatus direct na de eerste melding in Amber of Rood. Bekende kwaadaardige of onveilige websites worden gemarkeerd als Rood.
Hoe het werkt	De **Extension** kent een score toe aan de websites die je bezoekt: • Groen (OK) - score van 4 op 4: de website-eigenaar heeft een

	Extended Validation Certificaat uitgegeven door een Certificaat Autoriteit of de website-eigenaar is geregistreerd op atwork.Safeonweb.be (alleen voor Belgische organisaties). Daarom: Het zou in orde moeten zijn om verder te surfen op deze website. Het zou OK moeten zijn om gegevens te delen op deze website. • Amber (!) - scores van 1 tot 3 op 4: de eigenaar van de website heeft een Organisatie Validatie Certificaat, of een Domein Validatie Certificaat uitgegeven door een Certificaat Autoriteit, en de website is daarom niet geregistreerd op atwork.Safeonweb.be: Het zou in orde moeten zijn om verder te surfen op deze website. Als u twijfelt, kunt u beter geen gegevens delen op deze website. • Rood (X) - score van 0 uit 4: de website mist basisbeveiligingsfuncties of staat bekend als kwaadaardig. De eigenaar van de website heeft geen certificaat en is daarom niet gevalideerd. Daarom: We raden af om op deze website te surfen en gegevens te delen. Deze score is gebaseerd op drie variabelen; De **Certificaattype Score**, die het validatieniveau weergeeft van het Certificaat dat u voor uw Website heeft verkregen. Deze score wordt als volgt berekend; • 3/3 als u een willekeurig type certificaat hebt verkregen en uw website hebt geregistreerd op het Safeonweb@work-portaal of als u een Extended Validation-certificaat hebt verkregen; • 2/3 als je een Organisatie Validatie Certificaat hebt behaald; • 1/3 als u een Domein Validatie Certificaat heeft verkregen; of, • 0/3 als u geen enkel type certificaat voor uw website hebt. De **Certificate Authority score** is een score van 1 of 0, afhankelijk van of de Certificate Authority die het certificaat voor uw website heeft geleverd een bekende speler op de markt is en voorkomt in de databases van de CCB. De **domeinscore** geeft aan of uw domein als kwaadaardig is geregistreerd. In dat geval wordt uw totale score verlaagd naar 0.
Cijfers	Aangezien dit project op het moment van schrijven pas een maand geleden is gelanceerd, zijn de cijfers beperkt. Van oktober 2023 tot eind november werd de plugin (12000+) keer gedownload.

Disclaimer

Dit document en zijn bijlagen zijn opgesteld door het Centrum voor Cybersecurity België (CCB), een federale administratie opgericht bij Koninklijk Besluit van 10 oktober 2014 en onder de bevoegdheid van de Eerste Minister.

Het CCB aanvaardt geen verantwoordelijkheid voor de inhoud van dit document.

De verstrekte informatie:

- zijn uitsluitend van algemene aard en zijn niet bedoeld om rekening te houden met alle bijzondere situaties;
- zijn niet noodzakelijkerwijs volledig, nauwkeurig of actueel op alle punten;

Verantwoordelijke redacteur:
Centrum voor Cybersecurity België (CCB)
Dhr. De Bruycker, Algemeen Directeur
Wetstraat, 18
1000 Brussel

Wettelijk depot:
D/2024/14828/006