AGENTSCHAP VAN DE EUROPESE UNIE VOOR CYBERBEVEILIGING

EEN VERTROUWD EUROPA IN EEN VEILIGE CYBEROMGEVING

Enisa-strategie

juni 2020

EEN VERTROUWD EUROPA IN EEN VEILIGE CYBEROMGEVING

AGENTSCHAP VAN DE EUROPESE UNIE VOOR CYBERBEVEILIGING

VOORWOORD

Al meer dan 15 jaar speelt Enisa – het Agentschap van de Europese Unie voor cyberbeveiliging – een cruciale rol bij het realiseren van de ambitie van de EU om het vertrouwen in en de beveiliging van het digitale verkeer in heel Europa te versterken. Dat doet het samen met de lidstaten en de instellingen en agentschappen van de EU. Door gemeenschappen samen te brengen, heeft Enisa ertoe bijgedragen dat Europa goed is voorbereid op cyberincidenten en ook effectiever kan optreden als die zich voordoen.

Tegelijkertijd is de digitalisering van onze economie en samenleving enorm toegenomen. Dat blijkt des te meer nu we sinds het uitbreken van de COVID-19-crisis massaal onze toevlucht hebben genomen tot IT-oplossingen voor communicatie op afstand, om allerlei activiteiten gaande te houden. De crisis laat zien hoe sterk cyberaanvallers weten te profiteren van onze afhankelijkheid van deze technologieën. Ze toont ook aan hoe de cyberdreiging zich heeft verbreed, van gerichte aanvallen tot nieuwe vormen waarin miljoenen bedrijven en burgers tegelijkertijd worden bedreigd, waaronder een toenemend aantal geraffineerde aanvallen met gijzelsoftware. Daarnaast heeft de snelle ontwikkeling van digitale producten en diensten, van de cloud en videoconferenties tot 5G en kunstmatige intelligentie, voor nieuwe, al dan niet verhulde uitdagingen gezorgd.

Met zijn permanente mandaat en versterkte pakket van taken en vermogens is Enisa meer dan ooit de aangewezen partij om de EU en haar lidstaten te helpen het hoofd te bieden aan deze uitdagingen, nu er op het gebied van cyberbeveiliging in Europa een nieuw tijdperk aanbreekt.

Enisa vervult die leidende rol door in te spelen op relevante trends, en door actuele expertise en kennis te bevorderen en met alle betrokkenen te delen. Het agentschap ondersteunt de Europese Commissie en de lidstaten door zowel publieke en private actoren als burgers te helpen risico's in verband met cyberincidenten te voorkomen en te beheersen. Met de uitvoering van het kader voor cyberbeveiligingscertificering draagt Enisa bij aan een paradigmaverschuiving, door de beveiliging van digitale oplossingen die in Europa worden gebruikt, te verbeteren. Enisa vergroot daarbij de keuzemogelijkheden van alle betrokkenen, en versterkt hun vertrouwen. Het agentschap zal ook de Europese operationele gemeenschap voor cyberbeveiliging actief bijstaan, door nauw samen te werken en zich voor te bereiden op gezamenlijk optreden wanneer het volgende grootschalige incident zich voordoet.

In zijn nieuwe rol zal Enisa zich bij haar dagelijkse werkzaamheden laten leiden door de beginselen van openheid, wendbaarheid en betrouwbaarheid, en nauwer gaan samenwerken met de lidstaten en de Europese Commissie met het oog op de onderlinge afstemming van hun respectieve benaderingen. Verder zal Enisa ernaar streven om, in het kader van de huidige klimaatcrisis, de impact van zijn activiteiten op het milieu te verminderen en om als maatschappelijk verantwoorde werkgever een inclusieve werkomgeving te bieden.

In dit strategisch plan, dat is opgesteld met medewerking en bijdragen van alle medewerkers van Enisa, de leden van zijn raad van bestuur en zijn adviesgroep, worden heldere doelstellingen geformuleerd aan de hand waarvan Enisa de komende jaren aan de vele uitdagingen gaat werken.

Namens de raad van bestuur

Jean-Baptiste Demaison
voorzitter van de raad van bestuur

Krzysztof Silicki
vicevoorzitter van de raad van bestuur

VISIE

Een vertrouwd Europa in een veilige cyberomgeving

MISSIE

De missie van het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) is een hoog gemeenschappelijk cyberbeveiligingsniveau te bereiken in de hele Unie, in samenwerking met de bredere gemeenschap. Dat doet het agentschap door op te treden als expertisecentrum voor cyberbeveiliging, dat onafhankelijke en hoogwaardige technische adviezen en ondersteuning op cyberbeveiligingsgebied verzamelt en verstrekt ten behoeve van de lidstaten en instellingen van de EU. Het draagt bij aan de ontwikkeling en uitvoering van het cyberbeleid van de Unie.

Het is ons doel om het vertrouwen in de verbonden economie te versterken, de weerbaarheid en betrouwbaarheid van de infrastructuur en diensten van de Unie te vergroten en de digitale veiligheid van onze samenlevingen en burgers te waarborgen. Ons streven is een wendbare en maatschappelijk verantwoorde organisatie te zijn, die het milieu zo weinig mogelijk belast en gericht is op mensen.

WAARDEN

Gemeenschapsgericht
Enisa werkt met gemeenschappen van mensen. Het respecteert hun competenties en expertise, en bevordert synergieën en vertrouwen om zijn missie optimaal te verwezenlijken.

Excellente prestaties
Enisa streeft naar de meest actuele expertise in zijn werkzaamheden, houdt zich bij de uitvoering van die werkzaamheden aan de hoogste kwaliteitsnormen en evalueert zijn prestaties om die door middel van innovatie en anticipatie voortdurend te kunnen verbeteren.

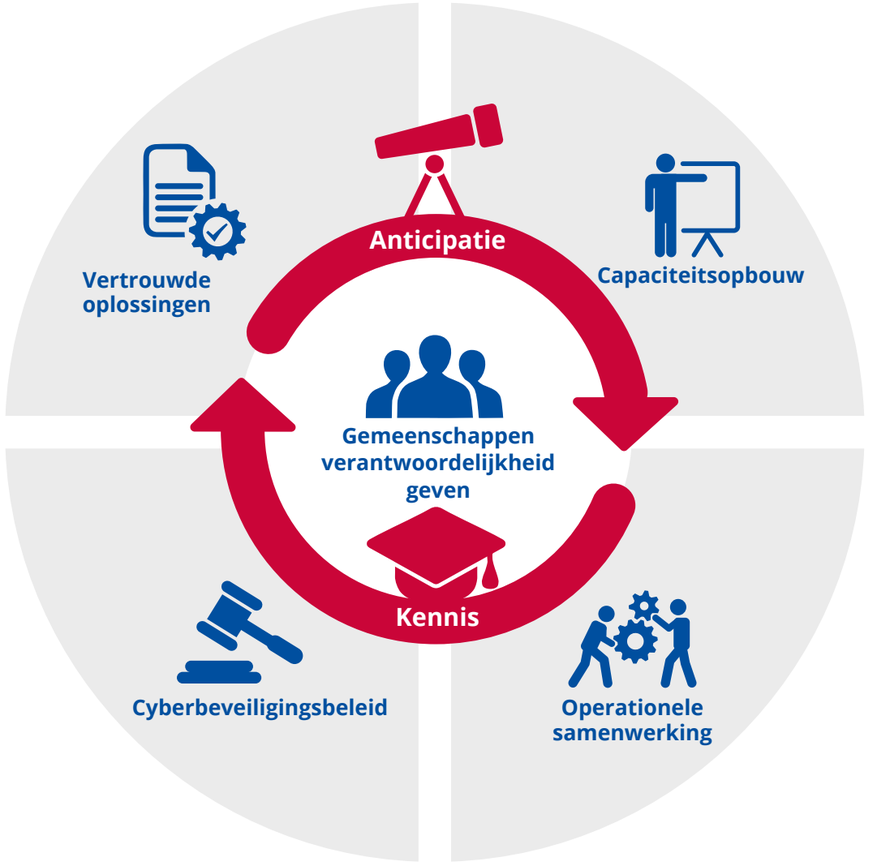
Integriteit/ethiek
Enisa houdt zich in zijn dienstverlening en werkomgeving aan ethische beginselen en voor de EU relevante regels en verplichtingen om eerlijkheid en inclusiviteit te waarborgen.

Respect
Enisa respecteert in zijn dienstverlening en werkomgeving de Europese grondrechten en fundamentele waarden, alsmede de verwachtingen van zijn belanghebbenden.

Verantwoordelijkheid
Enisa neemt verantwoordelijkheid en waarborgt aldus dat de beginselen ten aanzien van maatschappij en milieu in de praktijken en procedures worden geïntegreerd.

Transparantie
Enisa hanteert procedures, structuren en processen die open en onafhankelijk zijn en berusten op feiten, en beperkt aldus het risico van vooringenomenheid, dubbelzinnigheid, fraude en onduidelijkheid.

STRATEGISCHE DOELSTELLINGEN



SO1

Strategische doelstelling

“

BETROKKEN GEMEENSCHAPPEN MET VERANTWOORDELIJKHEDEN BINNEN HET GEHELE ECOSYSTEEM VOOR CYBERBEVEILIGING

Context

Cyberbeveiliging is een gedeelde verantwoordelijkheid. Europa streeft naar een sectoroverstijgend, geheel inclusief kader voor samenwerking. Enisa speelt een belangrijke rol bij het stimuleren van actieve samenwerking tussen alle belanghebbenden die in de lidstaten en binnen de EU-instellingen en -agentschappen bij cyberbeveiliging zijn betrokken. Het streeft ernaar te waarborgen dat al die inspanningen elkaar aanvullen. Daartoe zorgt het agentschap voor toegevoegde waarde voor de belanghebbenden, benut het kansen voor synergieën en weet het ook beperkte expertise en middelen voor cyberbeveiliging doelmatig in te zetten. Gemeenschappen moeten de bevoegdheid krijgen om het cybersecuritymodel op te schalen.

Wat wij willen bereiken

- Een geavanceerde, EU-brede kennisbank over concepten en praktijken op cyberbeveiligingsgebied, die samenwerking tussen de belangrijke actoren stimuleert, geleerde lessen en EU-expertise verspreidt en nieuwe synergieën creëert.
- Een ecosysteem voor cyberbeveiliging dat bestaat uit de autoriteiten van de lidstaten, de instellingen, agentschappen en instanties van de EU, verenigingen, onderzoekscentra en universiteiten, bedrijven, particuliere actoren en burgers, die alle hun eigen bijdrage leveren en verantwoordelijkheid dragen voor een cyberveilig Europa;

SO2

Strategische doelstelling

CYBERBEVEILIGING ALS INTEGRAAL ONDERDEEL VAN HET EU-BELEID

Context

De behoefte aan cyberbeveiliging - de hoeksteen van de digitale transformatie - werkt door in alle sectoren, en moet dan ook vanuit een breed beleidsperspectief (met bijbehorende initiatieven) worden benaderd. Het zou onwenselijk zijn als alleen een groep van gespecialiseerde technici en experts zich met cyberbeveiliging zou bezighouden. Het is daarom van belang dat cyberbeveiliging wordt verankerd als aandachtspunt in alle beleidsdomeinen van de EU. Het is van essentieel belang dat versnippering wordt vermeden en dat er een coherente aanpak wordt gevolgd, met inachtneming van de specifieke kenmerken van elke sector.

Wat wij willen bereiken

- Proactieve advisering en ondersteuning van alle relevante actoren op EU-niveau door middel van gerichte technische richtsnoeren, zodat cyberbeveiliging onderdeel wordt van de beleidsontwikkelingscyclus;
- Kaders voor het beheersen van cyberbeveiligingsrisico's, die in alle sectoren worden ingevoerd en gedurende de hele beleidscyclus voor cyberbeveiliging worden nageleefd.

SO3

Strategische doelstelling

> DOELMATIGE SAMENWERKING TUSSEN OPERATIONELE ACTOREN BINNEN DE UNIE WANNEER ZICH EEN GROOTSCHALIG CYBERINCIDENT VOORDOET

Context

Als wij de voordelen van de Europese digitale economie en samenleving optimaal willen benutten, moet de cyberbeveiliging gewaarborgd zijn. Cyberaanvallen kennen geen grenzen. Alle lagen van de samenleving kunnen worden getroffen. De Unie moet klaar staan om in het geval van een grootschalige en grensoverschrijdende cyberaanval of een cybercrisis onmiddellijk te kunnen optreden. Door de vele onderlinge afhankelijkheden over de grenzen heen is de behoefte aan effectieve samenwerking tussen de lidstaten en de EU-instellingen, met het oog op een snelle respons en juiste afstemming van de inspanningen op alle niveaus (strategisch, operationeel, technisch en qua communicatie), alleen maar duidelijker geworden.

Wat wij willen bereiken

- Voortdurende ondersteuning, tussen landen en tussen de verschillende lagen van de samenleving, voor samenwerking tussen de lidstaten en met de EU-instellingen. Steun voor de opschaling van technische, operationele, politieke en strategische samenwerking tussen de voornaamste operationele actoren, met name met het oog op eventuele grootschalige incidenten en crises, zodat een tijdige respons, uitwisseling van informatie, een goed overzicht van de situatie en effectieve crisiscommunicatie in de hele Unie gewaarborgd zijn;
- Brede en snelle technische verwerking van verzoeken van de lidstaten, om te kunnen voorzien in de technische en operationele behoeften in het kader van interventieprogramma's en crisisbeheersing.

SO4

Strategische doelstelling

GEAVANCEERDE COMPETENTIES EN CAPACITEITEN OP CYBERBEVEILIGINGSGEBIED IN DE HELE UNIE

Context

De frequentie en de complexiteit van cyberaanvallen nemen snel toe, terwijl ook het gebruik van ICT-infrastructuren en -technologieën door burgers, organisaties en bedrijven snel groeit. De behoefte aan kennis en competenties op cyberbeveiligingsgebied is groter dan het aanbod. De EU moet dan ook investeren in het bevorderen van vaardigheden en talent op dit gebied binnen de lidstaten, op alle niveaus - van de leek tot de hoogopgeleide specialist. Investeringen moeten niet alleen gericht zijn op het vergroten van de cybersecurityvaardigheden in de lidstaten, maar moeten er ook voor zorgen dat de verschillende operationele gemeenschappen over de juiste capaciteit beschikken om met cyberdreigingen om te gaan.

Wat wij willen bereiken

- Onderlinge afstemming van competenties op cyberbeveiligingsgebied, professionele ervaring en onderwijsstructuren om te kunnen voorzien in de voortdurend toenemende behoefte aan kennis en kunde op het gebied van cyberbeveiliging binnen de EU;
- Verhoogd bewustzijn van cyberbeveiliging en de desbetreffende competenties in de hele EU, en integratie van cyberkwesties als vast onderdeel van nieuwe disciplines;
- Gedegen en geteste vermogens met de capaciteit die nodig is om de toenemende dreiging in de hele EU het hoofd te bieden.

SO5

Strategische doelstelling

> STERK VERTROUWEN IN VEILIGE DIGITALE OPLOSSINGEN

Context

Digitale producten en diensten brengen zowel voordelen als risico's met zich mee; het is zaak die risico's goed in kaart te brengen en te verminderen. Bij het beoordelen van de veiligheid en het waarborgen van de betrouwbaarheid van digitale oplossingen is het van essentieel belang dat we een gezamenlijke aanpak volgen om zo de behoeften van de samenleving, markt, economie en cyberbeveiliging in balans te houden. Een neutrale en transparante entiteit draagt bij aan het vertrouwen onder consumenten in digitale oplossingen en de digitale omgeving in bredere zin.

Wat wij willen bereiken

- Een goed beveiligde cyberomgeving in de hele EU, waar burgers ICT-producten, -diensten en -processen kunnen vertrouwen, dankzij de inzet van certificeringsprogramma's op alle belangrijke technologische gebieden;

SO6

Strategische doelstelling

> INSPELEN OP OPKOMENDE EN TOEKOMSTIGE UITDAGINGEN OP CYBERBEVEILIGINGSGEBIED

Context

Tal van nieuwe technologieën die nu nog in hun kinderschoenen staan of juist op het punt staan gemeengoed te worden, zouden profiteren van een anticiperende methoden. Door middel van een gestructureerd proces dat een dialoog tussen de belanghebbenden mogelijk maakt, zouden besluitvormers en beleidsmakers in een vroeg stadium strategieën voor de beperking van de gevolgen kunnen vaststellen, zodat de EU weerbaarder wordt tegen cyberdreigingen en nieuwe uitdagingen beter het hoofd kan bieden.

Wat wij willen bereiken

- Inzicht in nieuwe trends en patronen door middel van prognoses en toekomstige scenario's, waarmee we de cyberuitdagingen van onze belanghebbenden kunnen beperken;
- Vroegtijdige beoordeling van de uitdagingen en risico's die voortvloeien uit de invoering van en aanpassing aan de nieuwe toekomstige opties, waarbij met de belanghebbenden wordt samengewerkt aan passende risicobeperkende strategieën.

SO7

Strategische doelstelling

> EEN EFFICIËNT EN DOELMATIG BEHEER VAN INFORMATIE EN KENNIS OP HET GEBIED VAN CYBERBEVEILIGING IN EUROPA

Context

Een effectieve cyberbeveiliging is afhankelijk van informatie en kennis. Om in deze constant veranderende digitale omgeving met steeds weer nieuwe actoren onze doelstellingen te kunnen bereiken, hebben cyberbeveiligingsprofessionals behoefte aan een doorlopend proces voor het verzamelen, organiseren, samenvatten, analyseren, communiceren en onderhouden van alle relevante informatie en kennis op het gebied van cyberbeveiliging. Alle fasen zijn essentieel om te waarborgen dat die informatie en kennis worden gedeeld en uitgebreid binnen het cyberbeveiligingsecosysteem in de EU.

Wat wij willen bereiken

- Een gezamenlijk beheer van informatie en kennis binnen het ecosysteem voor cyberbeveiliging in de EU in een toegankelijke, aangepaste en tijdige vorm, met gebruikmaking van een passende methodologie, infrastructuur en toolset, en met kwaliteitsborgingsmethoden die zorgen voor een voortdurende verbetering van de dienstverlening.

OVER ENISA

Het Agentschap van de Europese Unie voor cyberbeveiliging, Enisa, houdt zich bezig met het bereiken van een hoog niveau van cyberbeveiliging in heel Europa. Enisa is opgericht in 2004 en is versterkt door de cyberbeveiligingsverordening van de EU. Het agentschap draagt bij aan het cyberbeveiligingsbeleid van de EU, vergroot de betrouwbaarheid van ICT-producten, - diensten en -processen met certificeringsprogramma's voor cyberbeveiliging, werkt samen met lidstaten en instanties van de EU en helpt Europa zich voor te bereiden op de cyberuitdagingen van morgen. Door middel van kennisdeling, capaciteitsopbouw en bewustmaking werkt Enisa samen met zijn belangrijkste belanghebbenden om het vertrouwen in de verbonden economie te versterken, de veerkracht van de infrastructuur van de Unie te vergroten en uiteindelijk de Europese samenleving en burgers digitaal veilig te stellen. Zie voor meer informatie over Enisa en zijn werkzaamheden www.enisa.europa.eu

TP-02-20-759-NL-N

Enisa
Agentschap van de Europese Unie voor cyberbeveiliging

Kantoor Athene
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Griekenland

Kantoor Heraklion
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Griekenland

enisa.europa.eu