Nieuwe EU-cyberbeveiligingsstrategie en nieuwe regels om fysieke en digitale kritieke entiteiten weerbaarder te maken

Brussel, 16 december 2020

e Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid presenteren vandaag een nieuwe EU-cyberbeveiligingsstrategie. Die strategie is een essentieel onderdeel van de strategie om de digitale toekomst van Europa vorm te geven, het herstelplan voor Europa en de EU-strategie voor een veiligheidsunie. Ze zal de collectieve weerstand van Europa tegen cyberdreigingen versterken en ertoe bijdragen dat alle burgers en bedrijven ten volle van betrouwbare diensten en digitale instrumenten kunnen genieten. De Europeanen moeten geconnecteerde apparaten, het elektriciteitsnet, banken, vliegtuigen, overheidsdiensten en ziekenhuizen kunnen gebruiken in de wetenschap dat zij tegen cyberdreigingen worden beschermd.

Door de nieuwe cyberbeveiligingsstrategie kan de EU ook haar leiderschap op het vlak van internationale normen en standaarden in cyberspace versterken en intensiever samenwerken met partners over de hele wereld aan een mondiale, open, stabiele en veilige cyberspace die gebaseerd is op de rechtsstaat, de mensenrechten, de fundamentele vrijheden en de democratische waarden.

Voorts doet de Commissie voorstellen om kritieke entiteiten en netwerken beter bestand te maken tegen cyberdreigingen en fysieke dreigingen: een richtlijn inzake maatregelen voor een hoog gemeenschappelijk cyberbeveiligingsniveau in de Unie (herziene NIS-richtlijn of "NIS 2") en een nieuwe richtlijn voor de weerbaarheid van kritieke entiteiten. Die voorstellen bestrijken heel wat sectoren en hebben tot doel de huidige en toekomstige online en offline risico's, van cyberaanvallen en criminaliteit tot natuurrampen, op coherente en complementaire wijze aan te pakken.

Vertrouwen en veiligheid staan centraal in het digitale decennium van de EU

De nieuwe cyberbeveiligingsstrategie heeft tot doel een wereldwijd en open internet te waarborgen, en tegelijk de veiligheid te verzekeren en de Europese waarden en de grondrechten van iedereen te beschermen. Zij is gebaseerd op de verwezenlijkingen van de afgelopen maanden en jaren en bevat concrete voorstellen voor wetgeving, investeringen en beleid van de EU op drie gebieden:

1. **Weerbaarheid, technologische soevereiniteit en leiderschap**

De Commissie stelt voor de regelgeving inzake de beveiliging van netwerk- en informatiesystemen te hervormen in het kader van een richtlijn inzake maatregelen voor een hoog gemeenschappelijk cyberbeveiligingsniveau in de Unie (herziene NIS-richtlijn of "NIS 2"), zodat de cyberweerbaarheid van kritieke publieke en private sectoren wordt versterkt. Ziekenhuizen, energienetwerken, spoorwegen, datacentra, overheidsdiensten, onderzoekslaboratoria, productiecentra van kritieke medische apparatuur en geneesmiddelen en andere kritieke infrastructuur en diensten moeten ondoordringbaar blijven voor steeds sneller veranderende en complexere dreigingen.

De Commissie beveelt ook aan om in de hele EU een door artificiële intelligentie (AI) aangedreven netwerk van centra voor veiligheidsoperaties te bouwen. Dat zal een echt "cyberbeveiligingsschild" voor de EU vormen waarmee signalen van een cyberaanval vroegtijdig kunnen worden opgespoord en proactief maatregelen kunnen worden genomen om schade te voorkomen. Andere maatregelen zijn onder meer specifieke steun aan kleine en middelgrote ondernemingen in het kader van de digitale-innovatiehubs en meer inspanningen om de beroepsbevolking bij te scholen, het beste talent op het gebied van cyberbeveiliging aan te trekken en te behouden, en te investeren in open, concurrerende en op excellentie gebaseerde onderzoeks- en innovatieactiviteiten.

2. **Opbouw van operationele capaciteit om te voorkomen, te ontmoedigen en te reageren**

De Commissie werkt volgens een progressief en inclusief proces met de lidstaten aan een nieuwe gezamenlijke cybereenheid om de samenwerking te versterken tussen de EU-organen en de autoriteiten van de lidstaten die cyberaanvallen moeten voorkomen en ontmoedigen en daarop moeten reageren, zoals civiele en diplomatieke diensten en instanties voor rechtshandhaving en cyberdefensie. De hoge vertegenwoordiger doet voorstellen om het EU-instrumentarium voor

cyberdiplomatie te versterken, zodat kwaadwillige cyberactiviteiten die gevolgen hebben voor onze kritieke infrastructuur, toeleveringsketens en democratische instellingen en processen, worden voorkomen, ontmoedigd, belet en doeltreffend bestreden. De EU zal ook streven naar een betere samenwerking op het gebied van cyberdefensie en de ontwikkeling van geavanceerde cyberdefensiecapaciteit, voortbouwend op de werkzaamheden van het Europees Defensieagentschap. Zij zal de lidstaten aanmoedigen om de permanente gestructureerde samenwerking en het Europees Defensiefonds ten volle te benutten.

3. **Intensiever samenwerken voor een mondiale en open cyberspace**

De EU zal intensiever samenwerken met internationale partners om de op regels gebaseerde wereldorde te versterken, de internationale veiligheid en stabiliteit in cyberspace te bevorderen en de mensenrechten en fundamentele vrijheden online te beschermen. Zij zal met haar internationale partners in de Verenigde Naties en op andere relevante fora samenwerken om internationale normen en standaarden te ontwikkelen die de kernwaarden van de EU weerspiegelen. De EU zal haar instrumentarium voor cyberdiplomatie verder versterken en een EU-agenda voor de opbouw van de cybercapaciteit van derde landen opstellen. De cyberdialogen met derde landen, met regionale en internationale organisaties en met de multistakeholdergemeenschap zullen worden geïntensiveerd. De EU zal ook een wereldwijd EU-netwerk voor cyberdiplomatie creëren om haar visie op cyberspace te promoten.

Zij is vastbesloten om de nieuwe cyberbeveiligingsstrategie te ondersteunen met nooit eerder geziene investeringen in de digitale transitie. Daarvoor zal de komende zeven jaar een beroep worden gedaan op de langetermijnbegroting van de EU, met name via de programma's Digitaal Europa en Horizon Europa, en het herstelplan voor Europa. De lidstaten worden aangemoedigd om de EU-faciliteit voor herstel en veerkracht ten volle te benutten om de cyberbeveiliging te verhogen en de investeringen van de EU te evenaren. Het doel is te komen tot 4,5 miljard euro aan gecombineerde investeringen van de EU, de lidstaten en de sector, met name in het kader van het kenniscentrum voor cyberbeveiliging en het netwerk van coördinatiecentra, en te garanderen dat een groot deel daarvan naar kleine en middelgrote ondernemingen gaat.

De Commissie streeft er ook naar de industriële en technologische capaciteiten van de EU op het gebied van cyberbeveiliging te versterken, onder meer via projecten die gezamenlijk door de begrotingen van de EU en de lidstaten worden ondersteund. Dit is voor de EU een unieke kans om haar troeven te bundelen, en zo haar strategische autonomie te vergroten en haar leiderschap op het gebied van cyberbeveiliging te versterken in de hele digitale toeleveringsketen (waaronder gegevens en clouddiensten, processortechnologie van de volgende generatie, ultraveilige connectiviteit en 6G-netwerken), overeenkomstig haar waarden en prioriteiten.

Cyberweerbaarheid en fysieke weerbaarheid van netwerken, informatiesystemen en kritieke entiteiten

De huidige EU-maatregelen voor de bescherming van essentiële diensten en infrastructuur tegen cyberrisico's en fysieke risico's moeten worden geactualiseerd. De cyberbeveiligingsrisico's blijven veranderen door de toenemende digitalisering en interconnectiviteit. Ook de fysieke risico's zijn complexer geworden sinds de vaststelling in 2008 van de EU-regels inzake kritieke infrastructuur, die momenteel alleen betrekking hebben op de energie- en vervoerssector. De herzieningen zijn gericht op het actualiseren van de regels volgens de logica van de EU-strategie voor de veiligheidsunie, het opheffen van de valse tweedeling tussen online en offline en het doorbreken van het hokjesdenken.

Om het hoofd te bieden aan de toenemende dreigingen als gevolg van digitalisering en interconnectiviteit, zal de voorgestelde **richtlijn inzake maatregelen voor een hoog gemeenschappelijk cyberbeveiligingsniveau in de Unie (herziene NIS-richtlijn of "NIS 2")** middelgrote en grote entiteiten uit een groter aantal sectoren bestrijken op basis van hun kritieke karakter voor de economie en de samenleving. De herziene richtlijn verstrengt de beveiligingsvoorschriften die aan ondernemingen worden opgelegd, pakt de beveiliging van toeleveringsketens en betrekkingen tussen leveranciers aan, stroomlijnt de rapportageverplichtingen, voert strengere toezichtsmaatregelen voor nationale autoriteiten en strengere handhavingsvereisten in en streeft naar de harmonisatie van sanctieregelingen in de lidstaten. De voorgestelde NIS 2 zal bijdragen tot meer informatie-uitwisseling en samenwerking op het gebied van cybercrisisbeheer op nationaal en EU-niveau.

De voorgestelde **richtlijn inzake de weerbaarheid van kritieke entiteiten (CER)** breidt zowel het toepassingsgebied als de diepgang van de richtlijn Europese kritieke infrastructuur van 2008 uit. Ze omvat nu tien sectoren: energie, vervoer, banken, financiële marktinfrastructuren, gezondheid, drinkwater, afvalwater, digitale infrastructuur, openbaar bestuur en ruimtevaart. Op grond van de voorgestelde richtlijn zouden de lidstaten elk een nationale strategie vaststellen om de weerbaarheid

van kritieke entiteiten te waarborgen, en regelmatig risicobeoordelingen uitvoeren. Die beoordelingen zouden ook helpen bij het identificeren van een kleinere subgroep van kritieke entiteiten die onderworpen zouden zijn aan verplichtingen om hun weerbaarheid tegen niet-cyberrisico's te vergroten, zoals risicobeoordelingen op entiteitsniveau, het nemen van technische en organisatorische maatregelen, en incidentmeldingen. De Commissie zou op haar beurt aanvullende steun verlenen aan de lidstaten en kritieke entiteiten, bijvoorbeeld via een overzicht op Unieniveau van grensoverschrijdende en sectoroverschrijdende risico's, beste praktijken, methodologieën, grensoverschrijdende opleidingsactiviteiten en oefeningen om de weerbaarheid van kritieke entiteiten te testen.

Beveiliging van netwerken van de volgende generatie: 5G en daarna

In het kader van de nieuwe cyberbeveiligingsstrategie worden de lidstaten aangemoedigd om, met de steun van de Commissie en Enisa (Europees Agentschap voor cyberbeveiliging), de invoering te voltooien van de EU-5G-toolbox, een alomvattende en objectieve risicogebaseerde aanpak voor de beveiliging van 5G en de volgende generaties netwerken.

Volgens een vandaag gepubliceerd rapport over de impact van de aanbeveling van de Commissie inzake cyberbeveiliging van 5G-netwerken en de vooruitgang bij de invoering van het EU-instrumentarium van risicobeperkende maatregelen, liggen de meeste lidstaten sinds het voortgangsverslag van juli 2020 goed op schema om de aanbevolen maatregelen uit te voeren. Zij moeten er nu naar streven die uitvoering tegen het tweede kwartaal van 2021 af te ronden en te garanderen dat de vastgestelde risico's afdoende en op gecoördineerde wijze worden beperkt, met name om blootstelling aan hoogrisicoleveranciers tot een minimum te beperken en afhankelijkheid van die leveranciers te vermijden. De Commissie stelt vandaag ook de belangrijkste doelstellingen en acties vast om de gecoördineerde werkzaamheden op EU-niveau voort te zetten.

Leden van de Commissie aan het woord:

Margrethe **Vestager**, uitvoerend vicevoorzitter voor een Europa dat klaar is voor het digitale tijdperk: *"Europa zet zich in voor de digitale transformatie van onze samenleving en economie. Wij moeten die ondersteunen met nooit eerder geziene investeringen. De digitale transformatie versnelt, maar kan alleen slagen als personen en bedrijven erop kunnen rekenen dat de geconnecteerde producten en diensten waarop zij vertrouwen, veilig zijn."*

Josep **Borrell**, hoge vertegenwoordiger: *"Internationale veiligheid en stabiliteit zijn meer dan ooit afhankelijk van een mondiale, open, stabiele en veilige cyberspace waarin de rechtsstaat, de mensenrechten, de vrijheden en de democratie worden geëerbiedigd. Met deze strategie voert de EU haar inspanningen op om haar regeringen, burgers en bedrijven te beschermen tegen mondiale cyberdreigingen en om leiderschap te tonen in cyberspace, zodat iedereen de vruchten kan plukken van het internet en het gebruik van technologie."*

Margaritis **Schinas**, vicevoorzitter voor de bevordering van onze Europese levenswijze: *"Cyberbeveiliging is een centraal onderdeel van de veiligheidsunie. Er is geen onderscheid meer tussen dreigingen online en offline. De digitale en fysieke wereld zijn onlosmakelijk met elkaar verbonden. Uit deze reeks maatregelen blijkt dat de EU klaar is om al haar middelen en deskundigheid aan te wenden om zich met dezelfde vastberadenheid voor te bereiden en te reageren op fysieke dreigingen en cyberdreigingen."*

Thierry **Breton**, commissaris voor de Interne Markt: *"Cyberdreigingen veranderen snel en worden steeds complexer en flexibeler. Om te waarborgen dat onze burgers en infrastructuur worden beschermd, moeten wij een aantal stappen vooruit denken. Een weerbaar en autonoom Europees cyberschild betekent dat wij onze deskundigheid en kennis kunnen aanwenden om gevaren sneller op te sporen en te beantwoorden, potentiële schade te beperken en onze weerbaarheid te verhogen. Investeren in cyberbeveiliging betekent investeren in een gezonde toekomst voor onze online omgeving en in onze strategische autonomie."*

Ylva **Johansson**, commissaris voor Binnenlandse Zaken: *"Onze ziekenhuizen, afvalwatersystemen en vervoersinfrastructuur zijn slechts zo sterk als hun zwakste schakels. Verstoringen in een bepaald deel van de Unie kunnen elders gevolgen hebben voor de levering van essentiële diensten. Om de goede werking van de interne markt en de bestaansmiddelen van de inwoners van Europa te vrijwaren, moet onze belangrijkste infrastructuur bestand zijn tegen natuurrampen, terroristische aanslagen, ongevallen en pandemieën zoals wij er vandaag een meemaken. Dat is precies waar mijn voorstel inzake kritieke infrastructuur over gaat."*

Volgende stappen

De Europese Commissie en de hoge vertegenwoordiger zijn vastbesloten de nieuwe cyberbeveiligingsstrategie in de komende maanden uit te voeren. Zij zullen regelmatig verslag

uitbrengen over de geboekte vooruitgang, en het Europees Parlement, de Raad van de Europese Unie en belanghebbenden volledig op de hoogte houden van alle relevante acties en hen daarbij betrekken.

Het is nu aan het Europees Parlement en de Raad om de voorgestelde NIS 2-richtlijn en de richtlijn inzake de weerbaarheid van kritieke entiteiten onder de loep te nemen en goed te keuren. Zodra er overeenstemming is over de voorstellen en deze zijn aangenomen, moeten ze door de lidstaten binnen 18 maanden na de inwerkingtreding worden omgezet.

De Commissie zal de NIS 2-richtlijn en de richtlijn inzake de weerbaarheid van kritieke entiteiten periodiek evalueren en verslag uitbrengen over de werking ervan.

Achtergrond

Cyberbeveiliging is een van de topprioriteiten van de Commissie en een hoeksteen van een digitaal en geconnecteerd Europa. De toename van het aantal cyberaanvallen tijdens de coronacrisis heeft aangetoond hoe belangrijk de bescherming is van ziekenhuizen, onderzoekscentra en andere infrastructuur. Er zijn krachtige maatregelen nodig om de economie en de samenleving van de EU toekomstbestendig te maken.

De nieuwe cyberbeveiligingsstrategie stelt voor om cyberbeveiliging op te nemen in elk onderdeel van de toeleveringsketen, en om de activiteiten en middelen van de EU in de vier cyberbeveiligingsgemeenschappen (interne markt, rechtshandhaving, diplomatie en defensie) verder te bundelen. De strategie is gebaseerd op de strategie om de digitale toekomst van Europa vorm te geven en op de EU-strategie voor een veiligheidsunie, en steunt op een aantal wetgevingshandelingen, maatregelen en initiatieven die de EU heeft ingevoerd om de cyberbeveiligingscapaciteit te versterken en te zorgen voor een cyberbestendiger Europa. Het gaat onder meer om de cyberbeveiligingsstrategie van 2013, die in 2017 is herzien, en de Europese veiligheidsagenda 2015-2020 van de Commissie. Ook wordt erkend dat interne en externe veiligheid steeds meer met elkaar verbonden zijn, met name via het gemeenschappelijk buitenlands en veiligheidsbeleid.

De eerste EU-brede wetgeving inzake cyberbeveiliging, de NIS-richtlijn, die in 2016 in werking is getreden, heeft bijgedragen tot een hoog gemeenschappelijk beveiligingsniveau van netwerk- en informatiesystemen in de hele EU. Als onderdeel van haar belangrijke beleidsdoelstelling "Europa klaarmaken voor het digitale tijdperk" heeft de Commissie in februari van dit jaar een herziening van de NIS-richtlijn aangekondigd. Dankzij de EU-cyberbeveiligingsverordening, die in 2019 in werking is getreden, beschikt Europa over een kader voor cyberbeveiligingscertificering van producten, diensten en processen en is het mandaat van het EU-agentschap voor cyberbeveiliging versterkt.

Wat de cyberbeveiliging van 5G-netwerken betreft, hebben de lidstaten, met de steun van de Commissie en Enisa, een alomvattende en objectieve risicogebaseerde aanpak vastgesteld met de in januari 2020 aangenomen 5G-toolbox van de EU. De Commissie heeft haar aanbeveling over de cyberbeveiliging van 5G-netwerken uit maart 2019 geëvalueerd. Daaruit is gebleken dat de meeste lidstaten vooruitgang hebben geboekt bij de invoering van de toolbox.

Sinds de EU-strategie voor cyberbeveiliging van 2013 heeft de EU een samenhangend en holistisch internationaal cyberbeleid ontwikkeld. De EU heeft in samenwerking met haar partners op bilateraal, regionaal en internationaal niveau een wereldwijde, open, stabiele en veilige cyberspace gepromoot, gebaseerd op de kernwaarden van de EU en de rechtsstaat. De EU heeft derde landen ondersteund bij het vergroten van hun cyberweerbaarheid en hun vermogen om cybercriminaliteit aan te pakken. Zij heeft haar EU-instrumentarium voor cyberdiplomatie uit 2017 aangewend om verder bij te dragen tot de internationale veiligheid en stabiliteit in cyberspace, onder meer door voor het eerst sinds 2019 haar cybersanctieregeling toe te passen en acht personen en vier entiteiten en organen op een lijst te plaatsen. Ook op het gebied van samenwerking inzake cyberdefensie, onder meer wat betreft cyberdefensievermogen, heeft de EU aanzienlijke vooruitgang geboekt, in het bijzonder met haar beleidskader voor cyberdefensie (CDPF), de permanente gestructureerde samenwerking (PESCO) en de activiteiten van het Europees Defensieagentschap.

Ook in de volgende langetermijnbegroting van de EU (2021-2027) is cyberbeveiliging een prioriteit. In het kader van het programma Digitaal Europa zal de EU onderzoek, innovatie en infrastructuur op het gebied van cyberbeveiliging ondersteunen, evenals cyberdefensie en de Europese cyberbeveiligingssector. Omdat tijdens de lockdown steeds meer cyberaanvallen werden uitgevoerd, garandeert zij bovendien in het kader van het herstelplan voor Europa extra investeringen voor cyberbeveiliging als reactie op de coronacrisis.

De EU beseft al lang dat de weerbaarheid moet worden gewaarborgd van kritieke infrastructuur die essentiële diensten levert voor de goede werking van de interne markt en voor het dagelijkse leven en de bestaansmiddelen van de Europese burgers. Daarom heeft de zij in 2006 het Europees

programma voor de bescherming van kritieke infrastructuur (EPCIP) vastgesteld en in 2008 de richtlijn betreffende Europese kritieke infrastructuur (EBI) aangenomen, die van toepassing is op de energie- en de vervoerssector. Die maatregelen werden in de daaropvolgende jaren aangevuld met diverse sectorale en sectoroverschrijdende specifieke maatregelen, onder meer op het vlak van klimaatbestendigheid, civiele bescherming of buitenlandse directe investeringen.

Meer informatie

Factsheet over de nieuwe EU-cyberbeveiligingsstrategie

Factsheet over het voorstel voor een richtlijn inzake maatregelen voor een hoog gemeenschappelijk cyberbeveiligingsniveau in de Unie (herziene NIS-richtlijn)

Factsheet over cyberbeveiliging: extern optreden van de EU

Vragen en antwoorden: Nieuwe EU-cyberbeveiligingsstrategie en nieuwe regels om fysieke en digitale kritieke entiteiten weerbaarder te maken

Voorstel voor een richtlijn inzake maatregelen voor een hoog gemeenschappelijk cyberbeveiligingsniveau in de Unie (herziene NIS-richtlijn of "NIS 2")

Voorstel voor een richtlijn voor de weerbaarheid van kritieke entiteiten (zie ook bijlage 1 bij het voorstel, en de effectbeoordeling en de samenvatting daarvan)

Europese veiligheidsunie

Effectbeoordeling van de herziene NIS-richtlijn ("NIS 2")

Meer over cyberbeveiliging

Meer over de NIS-richtlijn

IP/20/2391

Contactpersoon voor de pers:

Johannes BAHRKE (+32 2 295 86 15)
Adalbert JAHNZ (+ 32 2 295 31 56)
Nabila MASSRALI (+32 2 298 80 93)
Marietta GRAMMENOU (+32 2 298 35 83)
Laura BERARD (+32 2 295 57 21)
Xavier CIFRE QUATRESOLS (+32 2 297 35 82)

Voor het publiek: Europe Direct per telefoon 00 800 67 89 10 11 of e-mail

Related media

Illustration 2020/2