DIGITALEUROPE

Omzetting van de EU-richtlijn inzake beveiling van netwerk- en informatiesystemen (NIS)

Brussel, 5 Juli 2016

SAMENVATTING

De Raad van de Europese Unie publiceerde op 21 april 2016 de nieuwe versie van de richtlijn inzake beveiling van netwerk- en informatiesystemen (NIS). Hoewel het Europees Parlement hem deze zomer nog officieel moet goedkeuren, gingen de drie EU-instellingen akkoord met de tekst en zal deze waarschijnlijk niet meer veranderen. De lidstaten moeten deze richtlijn binnen 21 maanden na zijn goedkeuring omzetten in nationale wetgeving. Ter ondersteuning van dit proces vindt u in bijlage de gids voor goede praktijken voor de implementatie van aspecten die relevant zijn voor de technologiesector en die de bedoelingen van de opstellers ook effectief waarmaken.

De NIB-richtlijn van de EU is de eerste pan-Europese wetgeving inzake cyberveiligheid en is gericht op de versterking van de cyberautoriteiten op nationaal niveau en de toename van de coördinatie tussen deze autoriteiten. Hij introduceert beveiligingseisen voor belangrijke industriële sectoren.

Nationale implementerende wetgeving mag de twee voornaamste doelstellingen van de richtlijn niet uit het oog verliezen: (1) de kritieke infrastructuur van het land een hoog niveau van cyberveiligheid garanderen; (2) een efficiënt samenwerkingsmechanisme in het leven roepen tussen EU-lidstaten om deze doelstelling te halen. De middelen moeten in de eerste plaats gaan naar het bereiken van deze twee belangrijke doelstellingen.

Voor de technologiesector zijn de bepalingen betreffende de zogenaamde digitaledienstverleners van bijzonder belang. De Richtlijn stelt duidelijk dat er een fundamenteel verschil is tussen aanbieders van essentiële diensten en digitale dienstverleners. Deze laatste worden namelijk niet als kritieke infrastructuren op zich beschouwd. De wetgeving erkent dat een incident met betrekking tot deze digitale diensten een aanzienlijk lager risiconiveau vertegenwoordigt voor de economische en openbare veiligheid van een land. Het behoud van dit onderscheid is cruciaal om de schaarse middelen van autoriteiten die moeten toezien op de regels en ze moeten afdwingen effectief en efficiënt in te zetten.

Daarom pleiten wij ervoor het beoogde toepassingsgebied van de betrokken diensten nauwlettend in de gaten te houden en vragen wij de beleidsmakers om alleen sectoren die als digitale dienstverlener of aanbieder van essentiële diensten worden geïdentificeerd in de nationale wetgeving beveiligingseisen op te leggen.

Wat rechterlijke bevoegdheid betreft, moeten digitale dienstverleners kunnen rekenen op de toepasselijke wet van het land waar hun hoofdkwartier is gevestigd, zelfs in gevallen waarbij bevoegde autoriteiten van meer dan een land zijn betrokken. Inzake toezicht, moeten de bevoegde autoriteiten kiezen voor een a-posterioriaanpak in plaats van toezicht op digitaledienstverleners algemeen te verplichten. Bovendien zouden ze zich moeten toespitsen op resultaten en het onderscheid bewaren tussen aanbieders van essentiële diensten en digitale dienstverleners door deze laatste niet te onderwerpen aan vereisten waarin de richtlijn niet voorziet, zoals auditing en bindende instructies.

DIGITALEUROPE
Wetenschapsstraat, 14 - 1040 Brussel
Tel. +32 (0) 2 609 53 10 Fax +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Lid van het transparantieregister voor de Commissie: 64270747023-20

De beveiligingsmaatregelen voor digitaledienstverleners zouden moeten verschillen van die voor aanbieders van essentiële diensten, aangezien de richtlijn stelt dat deze een veel lager veiligheidsrisico vertegenwoordigen. Besluitvormers moeten zich bewust zijn van het doel van de harmonisatie van deze diensten, ze moeten bestaande, door de industrie geleide internationale normen erkennen, technologiemandaten vermijden en het recht van de digitaledienstverleners respecteren dat in de richtlijn vervat zit om te kiezen voor de veiligheidsmaatregelen die het best aan hun systemen zijn aangepast. Incidentrapportage moet ook zo geharmoniseerd als mogelijk zijn op Europees niveau, zich toespitsen op incidenten die de continuïteit van de diensten beïnvloeden, de flexibiliteit in de meldingstijd respecteren en een vertrouwde omgeving creëren die het delen van informatie aanmoedigt zonder de meldende partij aan meer risico bloot te stellen.

De maatregelen die aan aanbieders van essentiële diensten zijn opgelegd zullen ook andere sectoren beïnvloeden aangezien veiligheidsmaatregelen en incidentrapportage naar beneden zullen doorstromen in de contractuele bepalingen. Dit geldt vooral voor cloudcomputerdiensten. Daardoor kunnen digitaledienstverleners onrechtstreeks onderworpen zijn aan de nationale wetgeving van hun klanten. Zij hebben er dus alle belang bij dat internationaal erkende beveiligingsmaatregelen op deze diensten van toepassing zijn. Wij stellen ook zoveel mogelijk coördinatie en synergieën voor tussen de rapportagevereisten voor aanbieders van essentiële diensten én digitaledienstverleners, aangezien deze laatste onderworpen kunnen zijn aan een dubbele kennisgeving.

De richtlijn vermeldt de ambitie om tot een hoger gemeenschappelijk niveau van beveiliging te komen van netwerken en informatiesystemen om de werking van de interne markt te verbeteren. Om dit hooggegrepen doel te bereiken, moeten de nationale omzettingen zich toespitsen op een risicogebaseerde, geharmoniseerde en internationale aanpak die de actoren van de privésector de flexibiliteit geeft om zich aan een voortdurend veranderend dreigingslandschap aan te passen, cyberautoriteiten in staat stelt beperkte middelen in te zetten op de grootste uitdagingen en erkent dat de oplossing voor een grenzeloos probleem globaal moet zijn. Wij hopen dat deze gids een handig hulpmiddel is om dat te bereiken en beantwoorden met plezier alle vragen die u nog heeft.

DIGITALEUROPE
Wetenschapsstraat, 14 - 1040 Brussel
Tel. +32 (0) 2 609 53 10 Fax +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Lid van het transparantieregister voor de Commissie: 64270747023-20

Bijlage: gids voor goede praktijken voor de implementatie van de NIB-richtlijn

1. Digitaledienstverleners

a) Toepassingsgebied

- De richtlijn bepaalt dat onlinemarktplaatsen, onlinezoekrobots en cloudcomputerdiensten als digitaledienstverleners moeten worden beschouwd en dus binnen het toepassingsgebied van de richtlijn moeten liggen. Hoewel het een richtlijn voor minimumharmonisatie (artikel 2) betreft, is het belangrijk doorheen de EU een zekere consistentie te handhaven. Lidstaten mogen in hun nationale wetgeving dus geen andere sectoren aan beveiligingseisen onderwerpen dan deze die geïdentificeerd zijn als digitaledienstverleners of aanbieders van essentiële diensten – zoals gedefinieerd in artikel 3.

- De richtlijn stelt uitdrukkelijk dat hardwarefabrikanten en softwareontwikkelaars geen aanbieders van essentiële diensten of digitaledienstverleners zijn en dus niet onderworpen mogen zijn aan de nationale wetgeving die de richtlijn implementeert (overweging 50).

- De richtlijn sluit onlinediensten die optreden als tussenpersonen voor diensten van derden waarbij uiteindelijk een verkoop- of serviceovereenkomst wordt afgesloten (bv. vergelijkingssites) uitdrukkelijk uit van het toepassingsgebied van onlinemarktplaatsen (overweging 50).

- Zoekfuncties die beperkt zijn tot de inhoud van een specifieke website mogen niet worden beschouwd als onlinezoekrobots, ook al maken ze gebruik van een externe provider (overweging 16).

- De definitie van een cloudcomputerdienst volgens de richtlijn is afhankelijk van het feit of computerbronnen door meerdere gebruikers worden gedeeld (artikel 4(19) en overweging 17). Aangezien privéclouds (in tegenstelling tot publieke clouds) tot één enkele organisatie behoren, moeten zij niet tot het toepassingsgebied behoren.

- De richtlijn benadrukt dat er fundamentele verschillen zijn tussen aanbieders van essentiële diensten en digitaledienstverleners. Daarom zijn digitaledienstverleners aan andere regels onderworpen (overweging 57). Dit onderscheid moet bij de implementatie van de richtlijn gehandhaafd blijven.

b) Rechterlijke bevoegdheid en toezicht

- De rechterlijke bevoegdheid voor digitaledienstverleners moet aan één enkele lidstaat worden verleend, waar de dienstverlener zijn voornaamste vestiging in de EU heeft. Deze komt in principe overeen met de plaats waar zijn hoofdkwartier in de EU is gevestigd (artikel 18.1 en overweging 64). Wij betogen dat digitaledienstverleners deze beslissing zelf mogen maken en dat ze alleen kan worden herzien indien bevoegde autoriteiten ze betwisten in geval van a-posteriori-supervisieactiviteiten.

- Wanneer digitaledienstverleners netwerk- en informatiesystemen hebben in andere landen dan waar hun hoofdkwartier is gevestigd, stelt artikel 17.3 dat de bevoegde autoriteiten moeten samenwerken. Vanuit het oogpunt van de digitaledienstverleners is het echter belangrijk dat de toepasselijke wetgeving

deze van het land van hun hoofdkwartier blijft en dat ze alleen rekenschap verschuldigd blijven aan de bevoegde autoriteit in dat rechtsgebied, die als hun tussenpersoon zal optreden.

- De richtlijn benadrukt dat digitaledienstverleners onderworpen zijn aan reactief a-posterioritoezicht en dat de bevoegde autoriteiten dus niet algemeen verplicht zijn om toezicht te houden op digitaledienstverleners. Ze mogen alleen actie ondernemen wanneer ze bewijs krijgen voorgelegd. (artikel 17.1 en overweging 60). Deze bepalingen moeten bij de implementatie van de richtlijn worden nageleefd.

- In tegenstelling tot aanbieders van essentiële diensten, kunnen de autoriteiten bij digitaledienstverleners alleen informatie vragen en eisen dat digitaledienstverleners eventuele gebreken oplossen. De richtlijn maakt duidelijk dat autoriteiten geen auditbevoegdheden hebben en geen bindende instructies kunnen uitvaardigen. Deze bepalingen moeten ook op nationaal niveau worden gerespecteerd.

c) Bijkomende eisen

- De beveiligings- en meldingseisen van digitaledienstverleners zijn onderworpen aan een maximumharmonisatie (artikel 16.10). Dit artikel moet van toepassing worden beschouwd op de producten, diensten en oplossingen waaruit hun netwerk- en informatiesystemen bestaan. Bijkomende bepalingen, zoals het testen van producten, zouden dus niet vereist moeten zijn in de mate dat de producten en diensten in deze context worden gebruikt.

d) Beveiligingsmaatregelen en -normen

- De beveiligingsmaatregelen voor digitaledienstverleners zouden lichter moeten zijn dan die voor aanbieders van essentiële diensten. Digitaledienstverleners moeten de vrijheid hebben om te bepalen hoe zij de beveiliging aanpakken en hoe zij hun netwerk- en informatiesystemen beschermen tegen de risico's waaraan ze blootgesteld zijn (overweging 49).

- De beveiligingsmaatregelen moeten procesgericht zijn en op risicobeheer focussen. Ze mogen niet eisen dat ICT-producten op een bepaalde manier worden ontworpen, ontwikkeld of vervaardigd (overweging 51).

- De richtlijn benadrukt dat lidstaten digitaledienstverleners geen verdere beveiligingseisen mogen opleggen (artikel 16.10).

- Toch verwachten we richtlijnen van verschillende actoren. De lidstaten zullen ervoor zorgen dat de maatregelen die in de richtlijn worden uiteengezet, worden toegepast (artikel 16.1), ze kunnen het gebruik van normen aanmoedigen om ze te implementeren (artikel 19.1) en de normen bespreken met Europese normalisatieorganisaties in de stuurgroep (artikel 11.3(h)). ENISA zal advies verstrekken over de geschikte normen (artikel 19.2) en de Europese Commissie is belast met het aannemen van uitvoeringshandelingen met betrekking tot de beveiligingsmaatregelen (artikel 16.8).

- Gezien deze complexiteit en de voordelen van harmonisatie, adviseren wij dat het nationale proces voornamelijk de uitvoeringshandelingen moet respecteren om geschikte maatregelen overeen te komen.

DIGITALEUROPE
Wetenschapsstraat, 14 - 1040 Brussel
Tel. +32 (0) 2 609 53 10 Fax +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Lid van het transparantieregister voor de Commissie: 64270747023-20

Dit proces moet in elk geval binnen een jaar na de goedkeuring van de richtlijn worden voltooid. De uitvoeringshandelingen zelf mogen geen afbreuk doen aan het vermogen van de digitaledienstverleners om te kiezen voor de beveiligingsmaatregelen die het meest geschikt zijn voor hun systemen.

- Het artikel over normen laat toe te verwijzen naar Europese of internationaal aanvaarde normen (artikel 19.1). Gezien de maturiteit van bestaande internationale normen op dit vlak, bevelen wij aan dat, wanneer de geschikte normen bestaan, de certificering tegen een van hen (zoals ISO 27001) moet volstaan om aan de vereisten te voldoen.

- In elke geval moet standaardcertificering optioneel zijn en niet verplicht. Artikel 19 benadrukt dat een norm alleen kan worden "aangemoedigd" en dat dit moet gebeuren "zonder het gebruik van een bepaald type technologie op te leggen of te bevoordelen."

e) Rapportage van beveiligingsincidenten

- Net als met de beveiligingsmaatregelen, spelen meerdere partijen een rol in de vormgeving van incidentrapportage onder de NIB-richtlijn. De lidstaten moeten ervoor zorgen dat digitaledienstverleners de beveiligingsincidenten melden die een aanzienlijke impact hebben op de diensten (die zich binnen het toepassingsgebied van de richtlijn bevinden) die zij verlenen (artikel 16.3), de stuurgroep is belast met de bespreking van de modaliteiten voor meldingen (artikel 11.3(m)) en de Commissie met de goedkeuring van uitvoeringshandelingen (artikel 16.8 en 9).

- Opnieuw bevelen wij aan dat bij de nationale omzetting de uitvoeringshandelingen worden gerespecteerd, waarvan de uitvoeringshandeling over de meldingsdrempel binnen een jaar na de voltooiing van de richtlijn moet worden aangenomen.

- Wat de types te rapporteren incidenten betreft, worden digitaledienstverleners belast met de melding van "elk incident dat een aanzienlijke impact heeft op de verlening van [hun] diensten" (artikel 16.3). Wat de implementatie van gelijkwaardige bepalingen voor telecomoperatoren onder artikel 13a van de kaderrichtlijn betreft, zijn we van mening dat deze moet worden geïnterpreteerd met de focus op **continuïteit (of beschikbaarheid)** van de verleende diensten. Met andere woorden, pannes die een bepaalde drempel bereiken (te bepalen via de uitvoeringshandelingen) moeten eerder worden gerapporteerd dan elk ander type beveiligingsincident. Het voordeel hiervan is dat de focus ligt op incidenten die het meest waarschijnlijk een impact hebben op de economie of de samenleving terwijl overlappingen met de meldingsvereisten voor inbreuken in verband met persoonsgegevens die voortvloeien uit de algemene verordening gegevensbescherming tot een minimum worden beperkt (hoewel niet volledig uitgesloten).

- Bovendien specificeert de meldingsplicht voor "aanbieders van essentiële diensten" dat deze aanbieders "incidenten die een aanzienlijke impact hebben op de continuïteit van de essentiële diensten die ze verlenen" zullen melden. Daarbij ligt de focus opnieuw duidelijk op de continuïteit (of beschikbaarheid) van diensten. De medewetgevers kwamen overeen dat de verplichtingen voor digitaledienstverleners lichter moeten zijn dan voor aanbieders van essentiële diensten (zie overweging 49). De verplichting inzake incidentrapportage voor digitaledienstverleners onder NIB mag niet ruimer zijn dan die voor aanbieders van essentiële diensten. Wat de drempels betreft, mag ze zelfs nog worden ingeperkt. Dit benadrukt opnieuw dat incidentrapportage voor digitaledienstverleners moet worden beperkt tot

incidenten die een bepaalde drempel bereiken en de continuïteit/beschikbaarheid van de diensten aantasten en geen incidenten betreft die betrekking hebben op de integriteit of vertrouwelijkheid van de gegevens die in ruime mate reeds worden gedekt door aanverwante meldingsvereisten onder de algemene verordening gegevensbescherming en de eIDAS-verordening.

- Wat de meldingstijd betreft, stellen wij de flexibiliteit op prijs die de formulering "onverwijld" voor de rapportage inhoudt (artikel 16.3). De implementatie mag niet leiden tot strikte deadlines aangezien incidenten aanzienlijk kunnen variëren qua complexiteit. Uniforme meldingstijden zouden onnauwkeurige rapportage in de hand werken wanneer de omvang van de getroffen systemen in eerste instantie nog onduidelijk is en zou het vermogen aantasten van de professionals in de reactie op incidenten om prioriteit te geven aan de reactie op het incident in plaats van de rapportage ervan.

- Zoals gezegd kunnen beveiligingsincidenten die volgens de richtlijn moeten worden gerapporteerd ook een kennisgeving vereisen volgens de wet op de gegevensbescherming, afhankelijk van het feit of er sprake is van een inbreuk op persoonsgegevens. Dat betekent niet alleen dat hetzelfde incident aan verschillende autoriteiten moet worden gemeld, maar dat deze autoriteiten zich zelfs in verschillende lidstaten kunnen bevinden, afhankelijk van de rechterlijke bevoegdheid die onder beide wetten van toepassing is op digitaledienstverleners. Wij bevelen lidstaten aan de nood te erkennen aan en te streven naar één enkele melding van incidenten en om communicatiekanalen proberen te creëren om relevante informatie onderling te delen, zonder afbreuk te doen aan de zakelijke vertrouwelijkheid.

- Bevoegde autoriteiten moeten rekening houden met implicaties op het vlak van reputatie en commerciële gevolgen voor digitaledienstverleners alvorens informatie over incidenten publiek te delen. Nog belangrijker is dat het onthullen van het incident het beveiligingsrisico kan vergroten. Daarom is het belangrijk om met de betrokken actoren te coördineren alvorens een incident bekend te maken.

- De richtlijn benadrukt dat informatie die vertrouwelijk wordt geacht als dusdanig moet worden behandeld (overweging 41, 59, artikel 1.5).

- Artikel 16.3 benadrukt dat de melding van een beveiligingsincident de meldende partij niet aan een groter risico mag blootstellen.

2. Aanbieders van essentiële diensten

a) Doorstroming van beveiligingsmaatregelen naar beneden toe

- Digitaledienstverleners die aanbieders van essentiële diensten als klant hebben, zullen onderworpen zijn aan toepasselijke beveiligingsmaatregelen die bij contractuele onderhandelingen doorstromen vanuit de statutaire verplichtingen voor aanbieders van essentiële diensten (artikel 14.1). Zij kunnen dus onrechtstreeks onderworpen zijn aan de nationale wetgeving van hun klanten, ongeacht de toepasselijke wet in het land van hun Europese hoofdkwartier.

- Daarom zouden inspanningen om de beveiligingsmaatregelen voor aanbieders van essentiële diensten te harmoniseren welkom zijn. Hoewel lidstaten het recht hebben om aanbieders van essentiële diensten strengere verplichtingen op te leggen dan de richtlijn oplegt (artikel 3), bevelen wij aan hiervan af te zien

en moedigen wij lidstaten aan naar een geharmoniseerde aanpak toe te werken. Dit kan door bij de nationale omzettingen bijkomende maatregelen te vermijden en in de stuurgroep te proberen geschikte beveiligingsmaatregelen te bepalen in plaats van te focussen op het nationale proces.

- De beveiligingseisen moeten zoveel mogelijk gebaseerd zijn op internationale normen (zoals de ISO 27x-reeks) en erkende goede beveiligingspraktijken.

- De beveiligingsmaatregelen die essentiëledienstverleners opgelegd krijgen mogen in geen geval eisen dat bepaalde ICT-producten op een bepaalde manier worden ontworpen, ontwikkeld of vervaardigd (overweging 51).

b) Doorstroming van de melding van beveiligingsincidenten naar beneden toe

- Aanbieders van essentiële diensten zijn verplicht om aan de digitaledienstverleners waarmee ze een contractuele relatie hebben beveiligingsincidenten te melden die de continuïteit van hun essentiële diensten kunnen beïnvloeden (artikel 16.5). Digitaledienstverleners zullen daarom contractueel verplicht zijn om aan de betrokken aanbieder van essentiële diensten de beveiligingsincidenten te melden die een impact op hen kunnen hebben.

- Wij stellen de flexibiliteit in meldingstijd voor digitaledienstverleners op prijs die de formulering “onverwijld” inhoudt (artikel 14.3). De nationale omzettingen mogen geen specifieke deadlines invoeren en in elk geval moet, indien aanbieders van essentiële diensten worden gevraagd om de tijd die ze nodig hadden voor de melding te rechtvaardigen, de periode waartegen ze worden beoordeeld van start gaan wanneer de aanbieder van essentiële diensten op de hoogte wordt gebracht van het incident, niet vanaf het moment dat de digitaledienstverlener zich ervan bewust is.

- Artikel 14.7 voorziet dat de stuurgroep richtlijnen opstelt over de meldingsomstandigheden in tegenstelling tot de harmoniserende rol van de Commissie voor meldingen van digitaledienstverleners. Gezien de dubbele meldingsvereiste voor digitaledienstverleners, is het belangrijk dat de respectievelijke meldingsvereisten niet tegenstrijdig zijn en zoveel mogelijk overeenstemmen. Dit proces moet dus worden afgetoetst aan deze doelstelling. Bovendien moeten de meldingsvereisten voor digitaledienstverleners de geheimhoudingsplicht respecteren die ze hebben tegenover hun klanten-aanbieders van essentiële diensten en mogen zij hen niet vragen om vertrouwelijke bedrijfsinformatie te delen.

DIGITALEUROPE
Wetenschapsstraat, 14 - 1040 Brussel
Tel. +32 (0) 2 609 53 10 Fax +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Lid van het transparantieregister voor de Commissie: 64270747023-20

OVER DIGITALEUROPE

DIGITALEUROPE vertegenwoordigt de digitale technologiesector in Europa. Tot onze leden behoren enkele van de grootste IT-, telecom- en consumentenelektronicabedrijven en nationale verenigingen uit elk deel van Europa. DIGITALEUROPE wil dat Europese bedrijven en burgers ten volle kunnen genieten van digitale technologie en willen dat Europa de beste digitaletechnologiebedrijven helpt groeien, aantrekt en behoudt.

DIGITALEUROPE zorgt ervoor dat de sector betrokken is bij de ontwikkeling en implementatie van het EU-beleid. Het ledenbestand van DIGITALEUROPE telt 62 leden uit de bedrijfswereld en 37 nationale vakorganisaties van over heel Europa. Op onze website kunt u terecht voor meer informatie over actualiteit en activiteiten: http://www.digitaleurope.org

LIDMAATSCHAP DIGITALEUROPE

Bedrijven

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies, ZTE Corporation.

Nationale vakverenigingen

België: AGORIA
Bulgarije: BAIT
Cyprus: CITEA
Denemarken: DI Digital, IT-BRANCHEN
Duitsland: BITKOM, ZVEI
Estland: ITL
Finland: FFTI
Frankrijk: AFNUM, Force Numérique, Tech in France
Griekenland: SEPE
Hongarije: IVSZ
Ierland: ICT IRELAND
Italië: ANITEC
Litouwen: INFOBALT
Nederland: Nederland ICT, FIAR
Oekraïne: IT UKRAINE
Oostenrijk: IOÖ
Polen: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Roemenië: ANIS, APDETIC
Slovenië: GZS
Slowakije: ITAS
Spanje: AMETIC
Turkije: Digital Turkey Platform, ECID
Verenigd Koninkrijk: techUK
Wit-Rusland: INFOPARK
Zweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Zwitserland: SWICO