Rijksdienst voor Ondernemend Nederland

Cybersecurity

Kansen voor het Nederlandse bedrijfsleven in België

>> Duurzaam, Agrarisch, Innovatief en Internationaal ondernemen

Inleiding

"*Om te kunnen groeien heeft de digitale economie vertrouwen en veiligheid nodig. Iedereen weet dat je in de fysieke wereld je voordeur beter op slot doet, maar hoe je dat in de online wereld doet, is voor veel mensen nog niet altijd duidelijk*" aldus de Belgische Minister van Digitale Agenda Alexander de Croo.[1]

Ons dagelijks leven speelt zich voor een steeds groter deel af in de digitale wereld. Deze digitalisering is een belangrijke drijfveer voor innovatie en economische groei, maar de risico's die zijn verbonden aan het gebruik van ICT zijn in de afgelopen jaren steeds duidelijker geworden.

Nederland heeft veel geïnvesteerd in de wijze waarop wordt ingespeeld op technologische trends en het effectief gebruik van ICT-middelen en vaardigheden. Mede daardoor is Nederland een internationaal internetknooppunt. Samen met Duitsland en het Verenigd Koninkrijk staat ons land in voor 18% van het wereldwijde internetverkeer.[2] Bovendien behoort Nederland in Europa tot de voorlopers op het gebied van cybersecurity. Nederland staat in 2017 op de 15e plek van de Global Cybersecurity Index (GCI).[3] De internationale ranglijst van de GCI bestaat uit 193 landen, die beoordeeld worden op onderdelen als nationaal beleid, juridische aanpak en de aanwezigheid en expertise van organisaties die zich bezighouden met cyberveiligheid.

België staat in 2017 op de 27e plaats van GCI ranglijst.[4] De Belgische cybersecurity-markt heeft zich de afgelopen jaren sterk ontwikkeld. In 2015 stond België nog op de 47ste plaats.

Conclusie (kansbeschrijving)

Twee derde van de Belgische bedrijven is in 2017 slachtoffer geworden van cybercriminaliteit. De toegenomen cyberaanvallen leidden tot meer investeringen in cybersecurity.[5] Bijna de helft van de Belgische bedrijven heeft in diezelfde periode hun financiële betrokkenheid bij de bestrijding van economische criminaliteit verhoogd. De Nederlandse expertise in de bestrijding van cybercriminaliteit biedt kansen voor grensoverschrijdende samenwerking tussen Nederland en België.

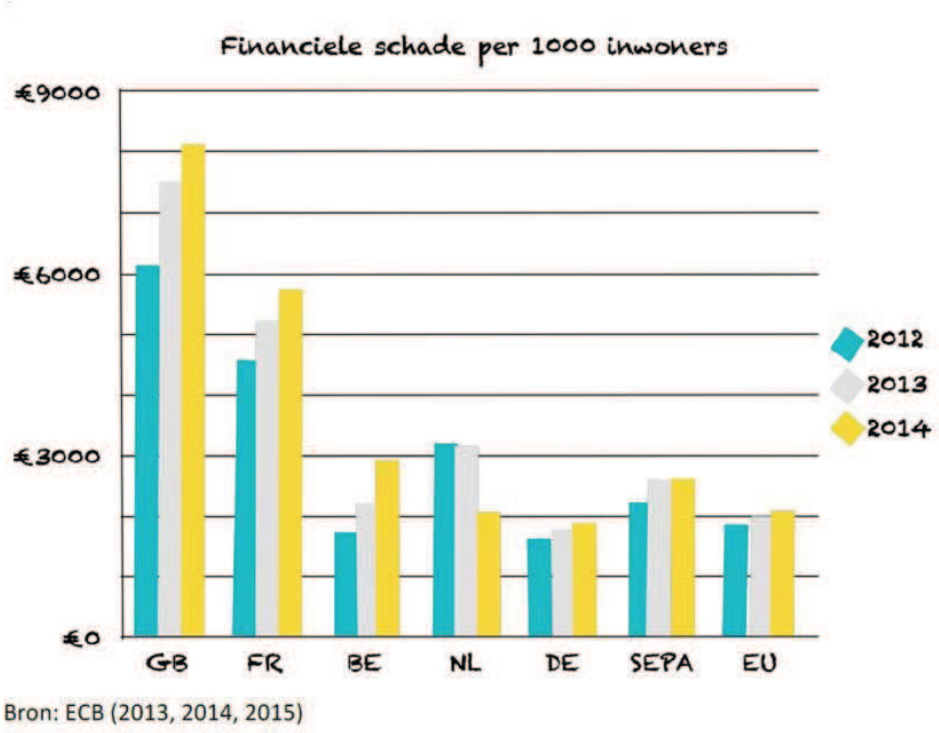
[1] http://www.decroo.belgium.be/nl/test-aankoop-en-google-willen-online-veiligheid-van-belgen-verbeteren-met-cybersimpelbe
[2] https://www.ncsc.nl/organisatie/nationale+cybersecurity+strategie
[3] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf
[4] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf
[5] https://www.pwc.be/en/news-publications/publications/2018/global-economic-crime-survey.html

Marktinformatie

1.1 Cybersecurity in België

In 2017 was de financiële schade als gevolg van cyberinbraken gelijk aan één procent van het Belgische bruto binnenlands product, een verlies van 4,5 miljard euro.[6]

De onderstaande grafiek geeft de ontwikkeling van financiële schade als gevolg van cybercrime in Europese landen weer.



Bron:http://www.seo.nl/uploads/media/201656_Economische_kansen_Nederlandse_Cybersecurity_sector.pdf (P.43)

Terwijl de financiële schade als gevolg van cybercrime in Nederland daalt, is er in België sprake van een stijgende financiële schade die ook boven het Europees gemiddelde ligt.

Het midden- en kleinbedrijf wordt meer geconfronteerd met cyberaanvallen. 60 procent van de cyberaanvallen in 2017 was gericht op het midden-en kleinbedrijf. Dit maakt België kwetsbaar omdat 95% van de ondernemingen geclassificeerd wordt als midden-en kleinbedrijf. Het federale Cyber Emergency team (CERT)

[6] http://datanews.knack.be/ict/nieuws/ccb-twee-derde-van-belgische-bedrijven-slachtoffer-van-cybercriminaliteit/article-normal-966793.html

ontvangt maandelijks 1000 tot 1500 meldingen van een cyberaanval waarbij het midden- en kleinbedrijf het doelwit van de cyberaanval is.[7]

Naast het aantal cyberaanvallen neemt ook het aantal gevallen van fraude met internetbankieren toe. 2017 is een recordjaar gebleken voor onlinebankfraude. Uit onderzoek van Febelfin, de overkoepelende organisatie van Belgische banken, blijkt dat bij de 3.205 gevallen van fraude via internetbankieren in totaal een bedrag van ruim 2,5 miljoen euro werd buitgemaakt, een gemiddelde van 787 euro per fraudegeval. Oorzaak van deze fraude is het toegenomen aantal phishingmails dat naar phishingsites wijst. Het aantal slachtoffers van phishing ligt in België hoger dan in andere Europese landen. Dit komt onder andere doordat België een meertalig land is. De phishing-mails die in Nederland en Frankrijk de ronde doen, komen allebei in België terecht. Daarnaast werden er tot 2017 geen grote campagnes gevoerd om de bevolking bewust te maken van de gevaren van phishingmails.[8]

1.1.1 Bedrijven

Voorheen werd verduistering van bedrijfsactiva aangemerkt als hoofdbedreiging, sinds 2016 is cybercriminaliteit het meest voorkomende type economische misdrijf waarmee de ondernemingen in België geconfronteerd worden. Uit de PWC Global Economic Crime and Fraud Survey 2018 blijkt dat bijna twee derde (65%) van de bedrijven in België in 2016 en 2017 slachtoffer werden van cybercriminaliteit, vergeleken met de helft (49%) wereldwijd.[9]

De meeste voorkomende vormen van cybercriminaliteit in 2017 zijn phishing (66 procent), malware (56 procent) en netwerkscannen (16 procent). Uit onderzoek van Belgian Cost of Crime (BCC) blijkt dat voor de meeste bedrijven de schade beperkt bleef tot een verstoring van de dagelijkse werking maar voor 9% van de door cyberafpersing en –chantage getroffen bedrijven liep de schade op tot meer dan 10.000 euro.[10]

Uit het onderzoek van PWC blijkt dat interne bedrijfscontroles de grootste (47%) bijdrage leveren aan de detectie van cyberaanvallen. Een groot deel van de economische criminaliteit (26%) wordt echter ook geconstateerd via externe tips.

De toegenomen cyberaanvallen in 2016 en 2017 leidden tot meer investeringen in cybersecurity.[11] Bijna de helft (47%) van de Belgische bedrijven heeft in diezelfde periode hun financiële betrokkenheid bij de bestrijding van economische criminaliteit verhoogd.

Bijna twee derde (62%) van de Belgische respondenten van het PWC onderzoek is van mening dat cybercrime de meest voorkomende economische misdaad zal blijven in de komende 24 maanden. Ondanks de toename van het aantal

[7] https://blog.axa.be/60-van-de-cyberaanvallen-zit-bij-kmos#

[8] https://www.tijd.be/ondernemen/banken/2017-recordjaar-voor-fraude-met-internetbankieren/9989176.html

[9] https://www.pwc.be/en/news-publications/publications/2018/global-economic-crime-survey.html

[10] https://bcc-project.be/surveys/wp4-2-the-impact-of-cybercrime-on-belgian.pdf

[11] https://www.pwc.be/en/news-publications/publications/2018/global-economic-crime-survey.html

cyberaanvallen is meer dan de helft van de Belgische PWC respondenten niet van plan de uitgaven in de komende twee jaar te verhogen.

De veiligheidsstrategie op het gebied van cybersecurity verschilt tussen grote en kleine bedrijven. Over het algemeen zijn de grote ondernemingen zich reeds bewust van de problematiek rond cyberveiligheid. Daarnaast zijn grote ondernemingen doorgaans beter uitgerust dan kleine ondernemingen om cyberaanvallen te weerstaan.

Het midden- en kleinbedrijf (MKB) vormt een kwetsbare groep voor cybercriminaliteit. Zij onderschatten vaak de mogelijke gevaren van cybercriminaliteit en de daaraan verbonden risico's. Daarnaast overschatten deze bedrijven vaak het eigen beveiligingssysteem. Er heerst een blind vertrouwen in die onderliggende infrastructuur en weinig interesse in de veiligheid daarvan. Ondanks dat midden- en kleinbedrijven steeds vaker het doelwit van aanvallen zijn, zijn veel bedrijven in 2018 nog niet bereid om middelen in te zetten of professionele hulp in te schakelen om de beveiligingsstrategie constant te actualiseren.

Midden- en kleinbedrijven zetten middelen tegen cyberaanvallen voornamelijk in als zij zijn getroffen door een cyberaanval, maar zij handelen niet preventief. Volgens Evoliris, het Brussels beroepenreferentie- centrum voor de ICT-sector, moet de focus van het MKB in België meer gericht zijn op preventieve maatregelen om het kwaad te bestrijden.[12] Vooral consultancybureaus die gespecialiseerd zijn in beveiliging maken een opmars in de markt door de grote behoefte. Met name het midden- en kleinbedrijf heeft behoefte aan de kennis en kunde van deze bedrijven.

Nederland draait op hoog niveau mee in cybersecurity. Nederland heeft de beste digitale infrastructuur van Europa, er is sprake van een aantrekkelijk vestigingsklimaat, Nederlanders zijn ICT minded en er is een hoogwaardige kennisinfrastructuur. Met universiteiten, kennisinstellingen, bedrijven en de overheid blinkt Nederland uit in de bestrijding van cybercrime.[13] Deze koppositie biedt kansen voor grensoverschrijdende samenwerking tussen Nederland en België.

1.1.2 Overheid

De Belgische overheid probeert door verschillende initiatieven het aantal cyberaanvallen te verminderen. Een belangrijk orgaan is het Centrum voor Cybersecurity België (CCB). Het CCB is het nationale centrum voor cyberveiligheid in België. Het doel van de CCB is het coördineren en het waken over de toepassing van de Belgische strategie omtrent cyberveiligheid. Het Belgische centrum kan vergeleken worden met het Nederlandse Nationaal Cyber Security Centrum dat in 2012 is opgericht.

Het in 2015 opgerichte Centrum voor Cybersecurity België is nog in volle opbouwfase maar heeft al verschillende initiatieven gerealiseerd. Met tips voor het ontwikkelen van een goede beveiligingsstrategie en het beheren van belangrijke

[12] http://www.evoliris.be/sites/default/files/publications/Cybers%C3%A9curit%C3%A9%20-%20rapport%20de%20veille%202017NL.pdf
[13] https://time.tno.nl/nl/artikelen/slagkracht-is-nodig-om-kansen-voor-cybersecurity-te-verzilveren/

data probeert de Belgische overheid bedrijven beter te wapenen tegen de impact van cybercriminaliteit. Door de hulpgids[14] gratis beschikbaar te stellen, hoopt de organisatie dat meer bedrijven tijd en budget willen investeren in de ontwikkeling van een cyberstrategie.

Het beheer van het federale cyber emergency team CERT.be is sinds januari 2017 overgedragen aan het CCB. De voornaamste taak van de CERT is informatie over veiligheidsincidenten inzamelen, deze informatie aan burgers en bedrijven doorgeven en hen adviseren.

Digital Transformation Office is verantwoordelijk voor digitale transformatie binnen de federale overheid, waarbij gebruiksvriendelijke en toegankelijke digitale dienstverlening centraal staan. Uit cijfers blijkt dat de digitale interacties tussen bedrijven en de overheid vanaf 2015 met meer dan vijftig procent zijn toegenomen.[15]

1.2 Bewustwording

Het CCB probeert bewustzijn te creëren door verschillende initiatieven. Zoals eerder vermeld introduceerde zij de online referentiegids die bedrijven informatie biedt voor een betere cyberveiligheidsstrategie. Daarnaast lanceerde zij in 2016 in samenwerking met de Cyber Security Coalition de grootste Belgische bewustwordingscampagne rond cyberveiligheid onder de slogan "6.491.641 miljoen Belgen helpen cybercriminelen." Het cijfer is afkomstig van een studie van de Universiteit Gent en slaat op het aantal mensen dat hun computer, tablet of smartphone onvoldoende of helemaal niet beveiligt. Ook is een groot offensief gestart tegen phishingmails. Internetgebruikers kunnen verdachte mails doorsturen om die te laten screenen door een IT-bedrijf.

De bewustzijnscampagnes gingen in Nederland eerder van start. In 2012 was er al de campagne Alert Online om de bewustwording op het gebied van cybersecurity te verhogen en online bewust gedrag te laten integreren in de levensstijl van mensen en organisaties.

Naast de initiatieven van de Belgische overheid zijn er ook private instanties die een bijdrage leveren aan de bewustwording in België:

- Belgian Cyber Security Convention (BCSC) 2018. BCSC probeert bedrijven meer bewust te maken door IT-specialisten uit het hele veld bij elkaar te brengen.
- Cyber Security Challenge Belgium 2018. De studentenwedstrijd is bedoeld om jongeren te stimuleren een carrière in cybersecurity te overwegen. De studententeams moeten binnen een bepaalde tijd uitdagingen uitvoeren op gebieden als cryptografie, netwerkbeveiliging en mobiele security. Zij hopen op deze manier een bijdrage te leveren aan een generatie van beveiligingsbewuste professionals en beveiligingsdeskundigen.

[14] https://cyberguide.ccb.belgium.be/nl

[15] http://www.digital.nl/nieuws/20171121-belgie-wordt-een-heus-digitaal-land

1.3 Onderzoek en Innovatie

1.3.1 Kennispotentieel

In België is er een groeiende kloof tussen het aanbod op de arbeidsmarkt en het stijgend aantal vacatures. Dit probleem wordt gedeeltelijk beïnvloed door het gebrek aan opleidingen in cyberveiligheid in België. De huidige opleidingen leveren niet voldoende experts in cybersecurity af om te kunnen voldoen aan de vraag van de sector.[16] Veel specialisten werkzaam in België zijn afkomstig uit het buitenland.

In 2020 zullen er naar verwachting bijna 230.000 ICT banen in België zijn. Dat zijn er 30.000 meer dan het aantal gekwalificeerde mensen. Het tekort wordt deels verklaard door de beperkte instroom vanuit technische opleidingen.

België kampt vooral met tekort aan hoogopgeleide cybersecurityexperts. Volgens de studie van Evoliris, het Brussels beroepenreferentiecentrum voor de ICT-sector, zal er tegen 2020 een tekort zijn van 2000 experts in cyberveiligheid.[17]

Ook de federale politie kampt met een groot gebrek aan computerspeurders. De Federal Computer Crime Unit (FCCU), belast met het bestrijden van computercriminaliteit, heeft niet voldoende personeel om de werkzaamheden uit te kunnen voeren.

Relevante evenementen/bronnen

2.1 Relevante organisaties

1. **Het Centrum voor Cybersecurity België**
   Het Centrum voor Cybersecurity België (CCB) is het nationale centrum voor cyberveiligheid in België. Het doel van de CCB is het coördineren en het waken over de toepassing van de Belgische strategie omtrent cyberveiligheid.
2. **Cyber security Coalition**
   De Cyber Security Coalition is een samenwerkingsverband van securityspecialisten uit overheidsorganisaties, bedrijven en de academische wereld die hun krachten bundelen in de strijd tegen cybercriminaliteit.
3. **KU Leuven Centre for IT and IP Law (CiTiP**)
   Het Centrum voor IT & IP Law is een onderzoekscentrum aan de Faculteit der Rechtsgeleerdheid van de Universiteit van Leuven (KU Leuven), met een staf van meer dan 40 onderzoekers gespecialiseerd in juridische en ethische aspecten van IT-innovatie en intellectueel eigendom.
4. **Computer Emergency Response Team**
   De voornaamste taak van de CERT is informatie over veiligheidsincidenten inzamelen, deze informatie aan burgers en bedrijven doorgeven en hen adviseren.

[16] http://www.evoliris.be/sites/default/files/publications/Cybers%C3%A9curit%C3%A9%20-%20rapport%20de%20veille%202017NL.pdf
[17] http://www.evoliris.be/sites/default/files/publications/Cybers%C3%A9curit%C3%A9%20-%20rapport%20de%20veille%202017NL.pdf

5. **CyberSecurity. Vlaanderen**
   Het is een samenwerkingsverband van een representatieve groep Vlaamse ondernemers actief in het domein van informatiebeveiliging en cybersecurity.
6. **BELTUG**
   Belgische vereniging van ICT-managers, met een focus op gespecialiseerde interne netwerken, mobiele communicatie, UC en Cloud. Directeur Danielle Jacobs IT Person of the Year 2018.

2.2 Evenementen en rapporten

De Nederlandse Ambassade in Brussel organiseert in samenwerking met handelsroute.nl en Digital Gateway een cybersecurity missie naar België van 25-27 juni 2018. Doel van deze missie het bijeenbrengen van bedrijven die zich bezighouden met cybersecurity. Centraal binnen deze missie staat het leren van elkaars best practices en grensoverschrijdende samenwerking om persoonlijke en zakelijke risico's te beperken.

Een groep van Nederlandse afgevaardigden uit de digitale infrastructuur en ICT zullen afreizen naar Brussel, om bedrijven te bezoeken, voor 1-op-1 introducties en het deelnemen aan ronde tafelsessies. Zowel beleidsmatige als commerciële oplossingen worden uitgewisseld. Deze missie is de eerste aanzet tot kennismaking en toekomstige samenwerking. Meer informatie vindt u op:www.handelsroute.nl/nl/s/BRU18

2.3 Handelsrelatie België-Nederland

België is na Duitsland de belangrijkste handelspartner van Nederland. Volgens de meest recente cijfers van het Centraal Bureau voor de Statistiek exporteerde Nederland in 2017 voor 43,6 miljard euro naar België en importeerde 37,9 miljard euro aan goederen en diensten.[18] Het merendeel van de export en import is voor Vlaanderen. Wallonië maakt recentelijk een voorspoedige ontwikkeling door, hierdoor wordt het in toenemende mate een kansrijke nabije markt. Brussel speelt een belangrijke rol door de aanwezigheid van de Europese instellingen, de NAVO en een tal van bedrijfszetels.

België is een federale staat waarbij de centrale overheid door verschillende staatshervormingen grote delen van haar bevoegdheid heeft afgestaan aan drie gewesten en drie gemeenschappen. Het Vlaamse, Waalse en Brussels Hoofdstedelijke Gewest zijn bevoegd voor o.a. economie en werkgelegenheid. Dat betekent dat voor een groot deel het economische beleid, de buitenlandse handel en het aantrekken van investeringen worden (uit)gevoerd door de individuele gewesten. De gemeenschappen zijn ingedeeld op basis van taal (Nederlands, Frans en Duits) en zijn bevoegd voor onder andere cultuur en onderwijs.

[18] https://www.rvo.nl/onderwerpen/internationaal-ondernemen/landenoverzicht/belgi%C3%AB/handel-en-economie

Contact

3.1 Dienstverlening Ambassade

Mocht u na het lezen van dit kans dossier enthousiast zijn geworden om België te gaan verkennen dan willen wij u het volgende adviseren. België is een land met andere manieren en gebruiken. Daarom is het aan te raden eerst met België kennis te maken, bijvoorbeeld door Belgische beurzen of voorlichtingsdagen te bezoeken. In de brochure “het gaat hier net even anders” leest u meer over de do's and don'ts voor succesvol zakendoen in België:
https://www.nederlandwereldwijd.nl/documenten/publicaties/2017/01/02/het-gaat-hier-net-even-wat-anders

De Nederlandse overheid biedt verschillende diensten aan om u te ondersteunen in het ondernemen in het buitenland. Mocht u nog vragen of opmerkingen hebben naar aanleiding van dit rapport aarzel dan niet om met de ambassade in Brussel contact op te nemen:

Ambassade van het Koninkrijk der Nederlanden
Economisch cluster
Kortenberglaan 4-10
B-1040 Brussel
Telefoon: 02-679.17.26
E-mail: bru-ea@minbuza.nl
www.nederlandwereldwijd.nl/landen/belgie

3.1.1 Aanspreekpunt

De ambassade is het aanspreekpunt voor individuele bedrijven. Het economisch cluster verstrekt actuele en betrouwbare informatie over het exporteren naar en investeren in de Belgische markt, informatie over de ontwikkelingen binnen kansrijke sectoren en over wet- en regelgeving. Ook wordt de ambassade ingeschakeld bij het oplossen van concrete problemen die het Nederlands bedrijfsleven in België ondervindt.

3.1.2 Handelsvragen

Op onze website vindt u informatie over tal van onderwerpen. Biedt de website geen antwoord op uw vraag, dan helpen wij u individueel verder. U kunt ons bereiken per email of telefoon.

3.1.3 Kansensignalering en handelsevenementen

De ambassade speurt continu naar marktkansen voor Nederlandse ondernemers. Dit doet zij door de ontwikkelingen op de Belgische markt nauwlettend te volgen. De marktkansen worden vertaald in berichten die gepubliceerd worden op onze website en op de website van RVO. Op basis van de kansensignalering organiseert de ambassade regelmatig handelsbevorderende activiteiten zoals informatiesessies, contactdagen, missies, matchmakings en evenementen.

3.1.4 Nieuwsbrief

De ambassade publiceert een digitale Economische Nieuwsbrief over marktevoluties, investeringsmogelijkheden en zakelijke opportuniteiten. U kunt zich kosteloos abonneren op de nieuwsbrief door een e-mail te sturen naar bru-ea@minbuza.nl. Tevens vindt u op de website het laatste nummer van de nieuwsbrief en een archief van de vorige nummers.

3.1.5 Zakenpartnerscan

Ziet u een kans op de Belgische markt voor uw bedrijf, maar zoekt u een handelspartner? Dan is de zakenpartnerscan iets voor u. De zakenpartnerscan is een persoonlijke introductie bij potentiële zakenpartners, speciaal voor ondernemers. Of u net komt kijken of al langer onderneemt in het buitenland, de zakenpartnerscan opent deuren naar distributeurs, importeurs, productiepartners of agenten in het buitenland. Aan dit instrument zijn kosten verbonden. De zakenpartnerscan wordt uitgevoerd in samenwerking met RVO. U kunt hiervoor een intakegesprek plannen bij RVO: https://www.rvo.nl/onderwerpen/internationaal-ondernemen/hoe-kan-rvonl-u-helpen-bij-zakendoen-het-buitenland

Colofon

Dit is een publicatie van:
RVO.nl
Prinses Beatrixlaan 2 / 2595 AL den Haag
Postbus 93144 / 2509 AC Den Haag
T +31 (0)88 0424242
E klantcontact@rvo.nl
www.rvo.nl

Dit is een publicatie van:

Rijksdienst voor Ondernemend Nederland
Postbus 93144 2509 AC Den Haag
www.rvo.nl