



Paper

Cybersecuritybedrijven in Nederland

CBS

Mei 2020

Inhoudsopgave

1. Inleiding	3
2. Methoden	4
2.1 Gebruikte eenheden	4
2.2 Webscrapen	4
2.3 Parsen	4
2.4 Voorselectie	4
2.5 Classificatie	5
2.6 Margeberekeningen	5
2.7 Handmatige controle	5
2.8 Correctie	6
2.9 Aantal domeinen	6
2.10 Koppeling bedrijfseconomische informatie	6
3. Resultaten	8
3.1 Aantal puur-cybersecuritydomeinen	8
3.2 Aantal gedeeltelijk-cybersecuritydomeinen	10
3.3 Bedrijfseconomische informatie puur-cybersecuritybedrijven	12
4. Beschouwing	14
4.1 Uitkomsten	14
4.2 Vervolg	14
 Bijlage I: Overzicht zoektermen gerelateerd aan cybersecurity	 15
 Bijlage II: Definitie cybersecurity	 16

1. Inleiding

Veilige en betrouwbare ICT is cruciaal voor de Nederlandse samenleving en economie. De toenemende afhankelijkheid van ICT maakt onze samenleving steeds kwetsbaarder. Digitale veiligheid, cybersecurity, is van essentieel belang. De Nederlandse Cybersecurity agenda (NCSA) bevat zeven focuspunten om die digitale veiligheid te waarborgen. Onder meer door voorop te lopen in het bevorderen van digitaal veilige hard- en software, het beschikken over weerbare digitale processen en het innemen van een toonaangevende positie op het gebied van kennis. In dit kader heeft het ministerie van Economische Zaken en Klimaat (EZK) het CBS gevraagd om te voorzien in bedrijfseconomische informatie over cybersecuritybedrijven in Nederland. Dergelijke informatie biedt handvatten voor beleidsontwikkeling en -monitoring van deze voor Nederland cruciale bedrijfstak.

Bedrijven die zich (deels) specialiseren in cybersecurity zijn op basis van de klassieke standaard bedrijfsindeling (SBI) niet specifiek te identificeren. Het gevolg hiervan is dat er slechts in beperkte mate kwantitatieve bedrijfseconomische gegevens over deze branche bekend zijn, omdat koppelingen met databronnen niet goed te maken zijn. Het CBS heeft daarom gebruik gemaakt van een methode, waarmee cybersecuritybedrijven op basis van *webdata* geïdentificeerd kunnen worden.

Binnen dit onderzoek zijn de onderstaande onderwerpen in kaart gebracht:

- aantal cybersecuritydomeinen (waarbij onderscheid naar puur en gedeeltelijk);
- ontwikkeling en niveau van omzet en werkzame personen bij puur-cybersecuritybedrijven.

2. Methoden

2.1 Gebruikte eenheden

In het onderzoek zijn verschillende soorten eenheden gebruikt om tot het eindresultaat te komen. Om het overzicht te bewaren wordt eerst kort ingegaan op hoe deze eenheden gedefinieerd zijn en hoe deze met elkaar in verband staan. De eenheden zijn:

- (web)domeinen: Websites die behoren bij bedrijven. Het is mogelijk dat één bedrijf meerdere domeinen heeft.
- Statistische eenheden/bedrijven: Ten behoeve van het maken van statistieken houdt het CBS statistische eenheden bij in het CBS-bedrijvenregister. Een statistische eenheid vertegenwoordigt een bedrijf¹. In dit artikel worden daarom de termen ‘bedrijf’ en ‘statistische eenheid’ door elkaar heen gebruikt.

Het verband tussen deze eenheden is dat het CBS domeinen heeft gekoppeld met statistische eenheden in het CBS-bedrijvenregister.

2.2 Webscrapen

De (web)domeinen binnen het niet-financiële bedrijfsleven² die in oktober 2019 bekend waren bij het CBS op basis van het CBS-bedrijvenregister en een levering van Dataprovider.com (circa 915 duizend unieke domeinen), vormen het uitgangspunt van dit onderzoek. Deze domeinen zijn gebruikt om met behulp van *webscrapen* maximaal 15 webpagina's per domein op te slaan. Bij *webscrapen* wordt in een automatisch proces een webpagina eenmalig en kort bezocht en informatie van de pagina gehaald.

2.3 Parsen

Bij het *parsen* zijn de opgeslagen webpagina's gecontroleerd op overbodige informatie. Hierbij zijn onder andere stopwoorden, interpunctie en HTML kop- en voettekst verwijderd. De opgeschoonde teksten zijn vervolgens opgeslagen als tekstbestanden.

2.4 Voorselectie

Om de onzekerheidsmarges op het aantal geïdentificeerde cybersecuritydomeinen te minimaliseren is uit de tekstbestanden van de vorige stap een voorselectie gemaakt. Deze voorselectie is gebaseerd op 80 zoektermen (zie bijlage I) die in verband staan met activiteiten die cybersecuritybedrijven kenmerken (zie de definitie van cybersecuritybedrijven in bijlage II). Hierdoor is de populatie van unieke domeinen

¹ Voor een verdere toelichting op hoe het CBS bedrijven middels statistische eenheden waarneemt, zie <https://www.cbs.nl/nl-nl/onze-diensten/methoden/begrippen?tab=b#id=bedrijf>

² Volgens de standaard bedrijvenindeling (SBI) de samentelling van hoofdstuk B-N, exclusief K en inclusief 95.

teruggebracht tot circa 46 duizend. Domeinen die niet één van deze termen gebruiken op hun webpagina's blijven in de vervolgstappen buiten beschouwing.

2.5 Classificatie

Het huidige onderzoek borduurt voort op de resultaten van een eerder onderzoek waarbij op regionaal niveau cybersecuritydomeinen zijn geïdentificeerd. Hiervoor werd een *machine learning* algoritme getraind dat bedrijven op basis van de informatie op hun webpagina kan classificeren: wel of geen cybersecuritybedrijf.

In dit onderzoek is het door het CBS ontwikkelde algoritme ingezet om de domeinen in de voorselectie te classificeren. Hierbij zijn er twee typen onderscheiden: *puur* en *gedeeltelijk*. *Puur-cybersecurity* heeft betrekking op domeinen waarbij het merendeel van de aanwezige tekst als cybersecurity geclassificeerd wordt en cybersecurity dus als hoofdactiviteit gezien kan worden. *Gedeeltelijk-cybersecurity* heeft betrekking op domeinen waarbij het merendeel of een deel van de aanwezige tekst als cybersecurity geclassificeerd wordt en cybersecurity dus als hoofd- of nevenactiviteit gezien kan worden.

Hiernaast is er met behulp van de statistische eenheden zoals die in oktober 2019 waren afgeleid binnen het CBS-bedrijvenregister onderscheid gemaakt in omvang: *groot* en *klein*. *Groot* heeft betrekking op domeinen die koppelen met statistische eenheden met 10 of meer werkzame personen. Domeinen die koppelen met statistische eenheden met minder dan 10 werkzame personen zijn gekenmerkt als *klein*.

De hierboven beschreven *machine learning* classificatie levert per type (*puur* en *gedeeltelijk*) en omvang (*groot* en *klein*) een waarde voor het aantal cybersecuritydomeinen (ml).

2.6 Margeberekeningen

Om rekening te houden met mogelijke fouten van het *machine learning* algoritme, is steekproefsgewijs de nauwkeurigheid van de classificatie bepaald. Hiermee is een reeks schattingen gemaakt voor het aantal cybersecuritydomeinen. Voor dit rapport worden de twee belangrijkste schattingen uitgelicht. De eerste is de *verwachte waarde* (*w*), het gemiddelde van de schattingen voor het aantal cybersecuritydomeinen. Daarnaast is er een *voorlopige 95%-bovengrens* (*vb*). Deze grens houdt rekening met de onzekerheid die rondom de schattingen van het aantal cybersecuritydomeinen kan liggen.

2.7 Handmatige controle

Alle positieve classificaties van het *machine learning* algoritme (ml) zijn vervolgens handmatig bekeken. Hierbij is er gecontroleerd op *vals positieven*, onterecht als cybersecurity geclassificeerde domeinen. Het resulterende aantal cybersecuritydomeinen wordt *handmatig bevestigd* genoemd.

2.8 Correctie

Voor een beperkt deel van het niet-financiële bedrijfsleven beschikt het CBS niet over het domein. Daarnaast blijkt een deel van de domeinen niet juist. Voor beide fouten en de *vals positieven* gevonden bij de hiervoor beschreven handmatige controle is een correctie op de *voorlopige 95%-bovengrens* (vb) uitgevoerd. Dit levert een *gecorrigeerde 95%-bovengrens* op.

2.9 Aantal domeinen

Om antwoord te geven op de vraag hoeveel cybersecuritydomeinen er per type en omvang zijn, wordt in eerste instantie uitgegaan van de *verwachte waarde* (w). Het verschil tussen het *handmatig bevestigde* aantal en de *verwachte waarde* (w) is het aantal cybersecuritydomeinen dat het CBS hoogstwaarschijnlijk heeft gemist, maar waarvan het niet weet welke het zijn.

De *gecorrigeerde 95%-bovengrens* is de grens waar met 95 procent zekerheid gezegd kan worden dat het aantal cybersecuritydomeinen onder ligt. Het verschil tussen het *handmatig bevestigde* aantal en de *gecorrigeerde 95%-bovengrens* is het aantal cybersecuritydomeinen dat het CBS in het slechtste (en meest onwaarschijnlijke) geval heeft gemist.

2.10 Koppeling bedrijfseconomische informatie

Om een verantwoorde koppeling met bedrijfseconomische informatie te kunnen maken zijn alleen statistische eenheden geselecteerd die uitsluitend koppelen met *puur-cybersecuritydomeinen* (statistische eenheden die ook koppelen met *gedeeltelijk cybersecurity* of andere domeinen zijn buiten beschouwing gelaten). Deze statistische eenheden zijn bestempeld als *puur-cybersecuritybedrijven*. Deze *puur-cybersecuritybedrijven* zijn gekoppeld aan omzet, werkzame personen en SBI. Doordat de afbakening heeft plaatsgevonden op gegevens verzameld in één periode (oktober 2019, zie 2.2) moet bij cijfers over eerdere jaren gerealiseerd worden dat bedrijven die voor het peilmoment waren opgeheven buiten beschouwing blijven.

2.10.1 Omzet

De omzetgegevens zijn uit de zogenoemde DRT-database van het CBS gehaald. De omzetten van de grootste bedrijven in deze database zijn verkregen door enquêtering. De omzetten van de overige bedrijven zijn gebaseerd op dataleveranties uit de btw-registratie van de Belastingdienst. Het zijn netto-omzetten: exclusief btw.

De omzetontwikkeling van de *puur-cybersecuritybedrijven* is gemeten door gebruik te maken van panels. Een bedrijf is lid van een panel als er een omzet beschikbaar is in beide bij de ontwikkeling betrokken jaren. Bij de berekening van de omzetontwikkeling wordt gebruik gemaakt van een jaar-op-jaarmutatie (JOJ). De omzetontwikkeling is een absolute omzetontwikkeling exclusief btw. Het is geen volume-ontwikkeling die gecorrigeerd is voor de prijsontwikkeling.

Het omzetniveau van de *puur-cybersecuritybedrijven* is per jaar vastgesteld door de omzet te sommeren over alle bedrijven, ongeacht of deze wel of niet in een panel zit. Daardoor zijn de cijfers niet één-op-één te vergelijken met cijfers over de omzetontwikkeling.

2.10.2 Werkzame personen

De werkzame personen zijn afkomstig uit het Bedrijfsdemografisch Kader (BDK). Dit is een register waarin de bedrijvenpopulatie van Nederland wordt bijgehouden, inclusief het aantal werkzame personen per bedrijf. Deze data is afkomstig uit de polisadministratie van het UWV. Bij bedrijven waar geen polisdata voor handen is, omdat er geen werknemers in dienst zijn, wordt op basis van de rechtsvorm een schatting gemaakt van het aantal werkzame personen.

De ontwikkeling en het niveau van het aantal werkzame personen van de *puur-cybersecuritybedrijven* wordt op dezelfde manier afgeleid als bij de omzet.

2.10.3 Standaard bedrijfsindeling (SBI)

De standaard bedrijfsindeling (SBI) is afkomstig uit het CBS-bedrijvenregister, zoals die in oktober 2019 bekend was bij het CBS.

3. Resultaten

3.1 Aantal puur-cybersecuritydomeinen

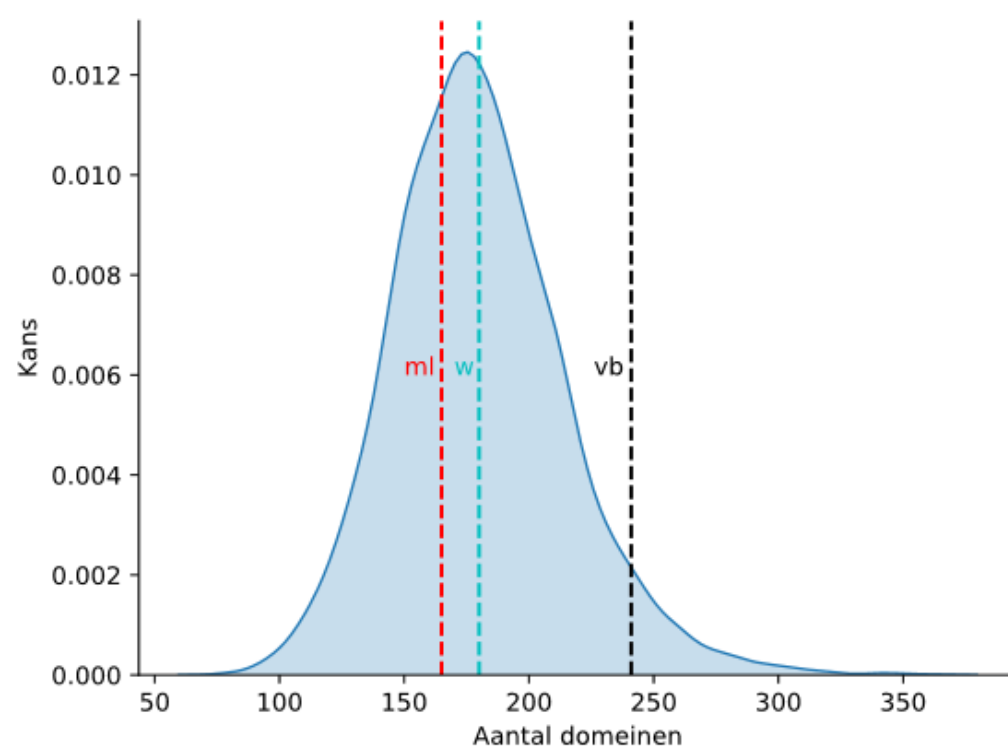
3.1.1 Groot

Tabel 1: uitkomsten margeberekening aantal grote puur-cybersecuritydomeinen in 2019

Machine learning classificatie (ml)	165
Verwachte waarde (w)	180
Voorlopige 95%-bovengrens (vb)	241

Bron: CBS

Figuur 1: uitkomsten margeberekening aantal grote puur-cybersecuritydomeinen in 2019



Bron: CBS

Tabel 2: uitkomsten handmatige controle en correctie aantal grote puur-cybersecuritydomeinen in 2019

Handmatig bevestigd	103
Gecorrigeerde 95%-bovengrens	194

Bron: CBS

Op basis van de bovenstaande uitkomsten is de verwachting dat er ongeveer 180 domeinen (w) zijn die als *groot* en *puur-cybersecurity* gekenmerkt kunnen worden. Hiervan

heeft het CBS 103 handmatig bevestigd. Waarschijnlijk zijn er dus ongeveer 80 domeinen gemist. In het slechtste (en meest onwaarschijnlijke) geval zijn er 95 domeinen gemist.

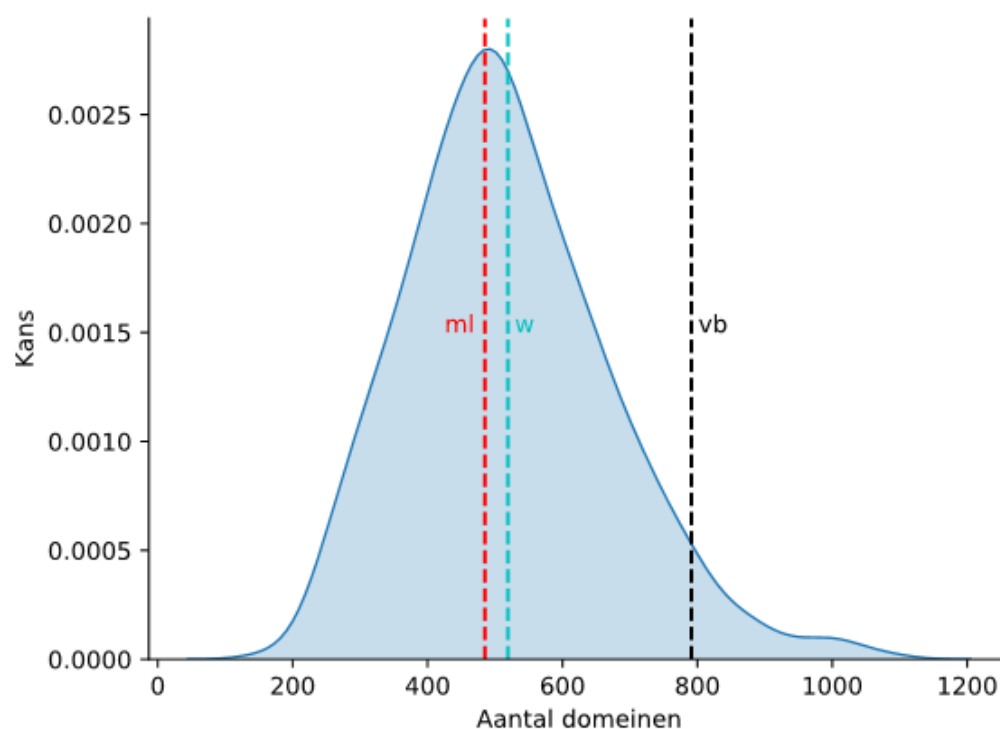
3.1.2 Klein

Tabel 3: uitkomsten margeberekening aantal kleine puur-cybersecuritydomeinen in 2019

Machine learning classificatie (ml)	485
Verwachte waarde (w)	519
Voorlopige 95%-bovengrens (vb)	799

Bron: CBS

Figuur 2: uitkomsten margeberekening aantal kleine puur-cybersecuritydomeinen in 2019



Bron: CBS

Tabel 4: uitkomsten handmatige controle en correctie aantal kleine puur-cybersecuritydomeinen in 2019

Handmatig bevestigd	342
Gecorrigeerde 95%-bovengrens	774

Bron: CBS

Op basis van de bovenstaande uitkomsten is de verwachting dat er ongeveer 519 domeinen (w) zijn die als *klein* en *puur-cybersecurity* gekenmerkt kunnen worden. Hiervan heeft het CBS 342 handmatig bevestigd. Waarschijnlijk zijn er dus ongeveer 177 domeinen gemist. In het slechtste (en meest onwaarschijnlijke) geval zijn er 432 domeinen gemist.

3.2 Aantal gedeeltelijk-cybersecuritydomeinen

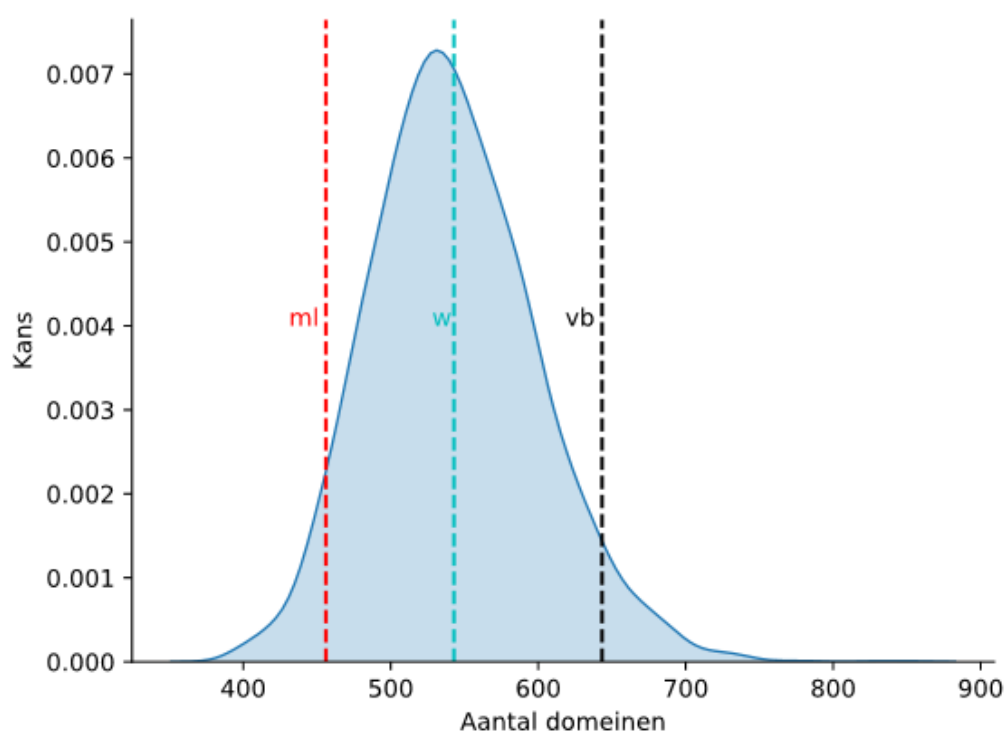
3.2.1 Groot

Tabel 5: uitkomsten margeberekening aantal grote gedeeltelijk-cybersecuritydomeinen in 2019

Machine learning classificatie (ml)	456
Verwachte waarde (w)	542
Voorlopige 95%-bovengrens (vb)	643

Bron: CBS

Figuur 3: uitkomsten margeberekening aantal grote gedeeltelijk-cybersecuritydomeinen in 2019



Bron: CBS

Tabel 6: uitkomsten handmatige controle en correctie aantal grote gedeeltelijk-cybersecuritydomeinen in 2019

Handmatig bevestigd	418
Gecorrigeerde 95%-bovengrens	581

Bron: CBS

Op basis van de bovenstaande uitkomsten is de verwachting dat er ongeveer 542 domeinen (w) zijn die als *groot* en *gedeeltelijk-cybersecurity* gekenmerkt kunnen worden. Hiervan heeft het CBS 418 handmatig bevestigd. Waarschijnlijk zijn er dus ongeveer 124 domeinen gemist. In het slechtste (en meest onwaarschijnlijke) geval zijn er 163 domeinen gemist.

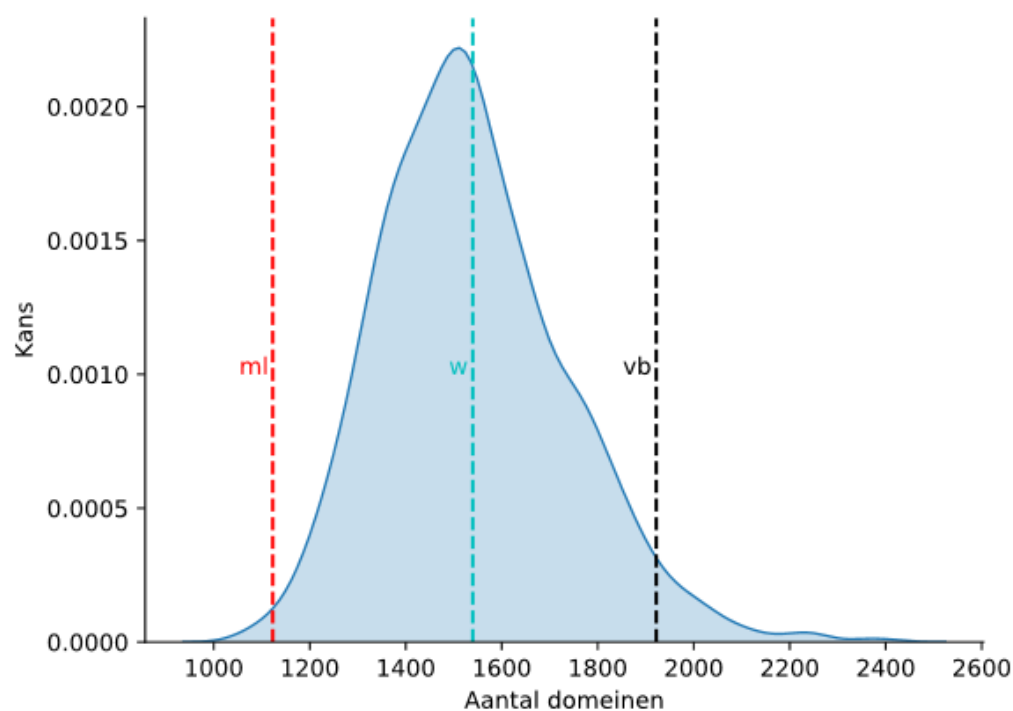
3.2.2 Klein

Tabel 7: uitkomsten margeberekening aantal kleine gedeeltelijk-cybersecuritydomeinen in 2019

Machine learning classificatie (ml)	1 123
Verwachte waarde (w)	1 540
Voorlopige 95%-bovengrens (vb)	1 922

Bron: CBS

Figuur 4: uitkomsten margeberekening aantal kleine gedeeltelijk-cybersecuritydomeinen in 2019



Bron: CBS

Tabel 8: uitkomsten handmatige controle en correctie aantal kleine gedeeltelijk-cybersecuritydomeinen in 2019

Handmatig bevestigd	1 056
Gecorrigeerde 95%-bovengrens	2 010

Bron: CBS

Op basis van de bovenstaande uitkomsten is de verwachting dat er ongeveer 1.540 domeinen (w) zijn die als *klein* en *gedeeltelijk-cybersecurity* gekenmerkt kunnen worden. Hiervan heeft het CBS 1.056 handmatig bevestigd. Waarschijnlijk zijn er dus ongeveer 484 domeinen gemist. In het slechtste (en meest onwaarschijnlijke) geval zijn er 954 domeinen gemist.

3.3 Bedrijfseconomische informatie puur-cybersecuritybedrijven

Voor de koppeling met bedrijfseconomische informatie zijn alleen statistische eenheden geselecteerd die uitsluitend koppelen met *puur-cybersecuritydomeinen*. Deze *puur-cybersecuritybedrijven* zijn gekoppeld aan omzet, werkzame personen en SBI. Dit waren uiteindelijk circa 80 bedrijven met 10 of meer werkzame personen en 330 bedrijven met minder dan 10 werkzame personen. Hieronder worden de jaar-op-jaar ontwikkelingen en het niveau van de omzet en werkzame personen, alsmede de SBI van de *puur-cybersecuritybedrijven* weergegeven.

3.3.1 Omzet

Tabel 9: jaar-op-jaar ontwikkelingen omzet van puur-cybersecuritybedrijven, naar bedrijfsomvang

	Totaal	Bedrijven met 10 of meer werkzame personen	Bedrijven met minder dan 10 werkzame personen
	%		
2017	1,2	1,4	-1,6
2018	9,1	8,8	14,3
2019	9,2	9,8	0,9

Bron: CBS

Tabel 10: omzetniveau³ van puur-cybersecuritybedrijven, naar bedrijfsomvang

	Totaal	Bedrijven met 10 of meer werkzame personen	Bedrijven met minder dan 10 werkzame personen
	Mln. euro's		
2016	1 000	935	65
2017	1 075	1 005	70
2018	1 185	1 095	90
2019	1 315	1 220	95

Bron: CBS

³ Afgerond op 5 mln. euro.

3.3.2 Werkzame personen

Tabel 11: jaar-op-jaar ontwikkelingen werkzame personen van puur-cybersecuritybedrijven, naar bedrijfsomvang

	Totaal	Bedrijven met 10 of meer werkzame personen	Bedrijven met minder dan 10 werkzame personen
	%		
2017	17,0	18,0	7,5
2018	12,8	13,3	7,8

Bron: CBS

Tabel 12: werkzame personen⁴ van puur-cybersecuritybedrijven, naar bedrijfsomvang

	Totaal	Bedrijven met 10 of meer werkzame personen	Bedrijven met minder dan 10 werkzame personen
	VTE		
2016	3 755	3 400	355
2017	4 460	4 045	415
2018	5 080	4 590	490

Bron :CBS

3.3.3 SBI

Tabel 13: Aantal puur-cybersecuritybedrijven per SBI sectie

Sectie	Omschrijving	Aantal
G	Handel	35
J	Informatie en communicatie	260
M	Specialistische zakelijke diensten	70
-	Overige secties	45

Bron :CBS

⁴ Afgerond op vijftallen

4. Beschouwing

4.1 Uitkomsten

Als gevolg van de gehanteerde aanpak wijken de uitkomsten van dit onderzoek af van reguliere CBS onderzoeken, waarbij de standaard bedrijfsindeling (SBI) wordt toegepast.

4.1.1 Aantallen

Om zoveel mogelijk aan te sluiten bij het niveau waarop het *webscrapen* wordt toegepast, hebben de aantallen betrekking op internetdomeinen in plaats van bedrijven. Wanneer de vertaling naar bedrijven zou worden gemaakt, zouden de aantallen waarschijnlijk lager uitvallen. Dit geldt met name voor grote bedrijven (10 of meer werkzame personen). Dergelijke bedrijven hebben vaker meerdere domeinen.

Daarnaast zijn de aantallen gebaseerd op een reeks van schattingen in plaats van een integrale telling. Dit is nodig om rekening te houden met de classificatiefouten die het *machine learning algoritme* kan maken (domeinen onterecht als cybersecurity classificeren).

4.1.2 Omzet en werkzame personen

Om een verantwoorde koppeling met bedrijfseconomische informatie te kunnen maken is bij de omzet en werkzame personen wel een vertaling naar bedrijven gemaakt. Hierbij zijn alleen statistische eenheden geselecteerd die uitsluitend koppelen met *puur-cybersecuritydomeinen* (statische eenheden die ook koppelen met *gedeeltelijk cybersecurity* of andere domeinen zijn buiten beschouwing gelaten). Deze statische eenheden zijn bestempeld als *puur-cybersecuritybedrijven*. De in het rapport gepresenteerde uitkomsten met betrekking tot omzet en werkzame personen dienen hierdoor geïnterpreteerd te worden als ondergrenzen voor *puur-cybersecuritybedrijven*.

4.2 Vervolg

Het huidige onderzoek vormt een goede basis om de cybersecuritysector in Nederland in kaart te brengen. Zoals hierboven beschreven is het aantal *cybersecuritydomeinen* binnen de afgebakende populatie geschat en de omzet en werkzame personen in kaart gebracht voor de *puur-cybersecuritybedrijven*. Een logische vervolgstap zou het beter duiden van het economische belang van de cybersecuritysector zijn. Het CBS ziet aanknopingspunten in het huidige onderzoek om in aanvulling op de reeds vastgestelde ondergrenzen net als bij de aantallen, schattingen te maken voor de omzet en werkzame personen binnen de afgebakende populatie.

Bijlage I: Overzicht zoektermen gerelateerd aan cybersecurity

hack	digitale dreiging
antivirus	digitale dreigingen
back-up	digitale identificatie
bedrijfsrecherche	digitale infrastructuur
beveiligingsprotocol	digitale sabotage
beveiligingsupdates	digitale veiligheid
blockchain	digitale verstoring
chantage	digitale weerbaarheid
computernetwerken	encryptie
cyber	end-point
cyberaanvallen	firewall
cyberconflicten	fraud
cybercrime	fraude
cybercriminaliteit	hacking
cyberdelicten	ICT-systeem
cyberpesten	ICTsystemen
cybersabotage	identiteitsfraude
cybersecurity	identity fraud
cybersecurity-dienstverlening	in de cloud
cybersecuritydomein	in the cloud
cyberspace	informatiebeveiliging
cyberspionage	informatiesystemen
cyberterrorisme	Internet of Things
cyberveilig	IT verstoring
cyberveiligheid	malware
cyberwarfare	netwerkbeveiliging
cyberweerbaarheid	Network access control
data distribution	network security
data distribution	oneigenlijk delven van
data protection	cryptomunten
data storage	online incident
datalek	phishing
datalekken	ransomware
DDoS	spam
delict	spionage
digitaal indicent	spying
digitale aanval	token-authenticatie
digitale bedrijfsgegevens	veiligheidstest
digitale beveiliging	verkoopfraude
digitale bewustwording	VPN
digitale data	

Bijlage II: Definitie cybersecurity

Het onderscheid tussen cybersecuritybedrijven en andere ondernemingen is gebaseerd op onderstaande omschrijving van cybersecurity:

- Bedrijven die werkzaam zijn op het gebied van ICT-beveiliging
- Bedrijven die afgeschermd serverruimte reserveren voor klanten
- Bedrijven die preventief optreden tegen cybercrime en tegen niet-strafbare cyberincidenten
- Bedrijven die cybersecurity-maatregelen treffen om schade, veroorzaakt door verstoring, uitval of misbruik van ICT te voorkomen en/of te herstellen. Deze maatregelen vallen uiteen in drie categorieën:
 - a. ICT-technisch:
 - i. Firewalls
 - ii. Antivirussoftware
 - iii. Beveiligingsprotocollen
 - b. ICT-organisatorisch:
 - i. Doorlooptijd van het repareren van kwetsbaarheden in software
 - ii. Gebruik van wachtwoorden of andere manieren van toegang tot een ICT-systeem
 - c. Alert maken/houden van bedrijven en/of particulieren:
 - i. Vergroten van kennis en bewustwording op het terrein van cybersecurity
 - ii. Aanreiken van makkelijk implementeerbare maatregelen/gedragingen

Colofon

Uitgever

Centraal Bureau voor de Statistiek
Henri Faasdreef 312, 2492 JP Den Haag
www.cbs.nl

Prepress

CCN Creatie en visualisatie

Ontwerp

Edenspiekermann

Inlichtingen

Vragen over deze publicatie kunnen gestuurd worden aan CBS onder vermelding van het referentienummer 305557. Ons e-mailadres is infoservice@cbs.nl.

© Centraal Bureau voor de Statistiek, Den Haag/Heerlen/Bonaire, 2020
Verveelvoudigen is toegestaan, mits het CBS als bron wordt vermeld