

Je bedrijfsnaam is van onschatbare waarde, ook online

Hoe je je merk online beschermt en versterkt



SIDN | 1 april 2023

Waarom dit whitepaper?

Dit whitepaper is voor ondernemers in het midden- en kleinbedrijf die online actief zijn.

Lees dit whitepaper als je wilt weten:

- Waarom online merkbescherming voor het mkb steeds belangrijker wordt;
- Wat de belangrijkste risico's zijn voor het mkb;
- Hoe je effectief omgaat met online merkinbreuk als je geen security-officer of bedrijfsjurist hebt.

Dit whitepaper word je aangeboden door SIDN

Wij zijn SIDN. Elke keer als jij een .nl-adres intypt, zorgen wij ervoor dat je bij de juiste site uitkomt. Want wij zijn de beheerder van het .nl-domein. We werken dus in het hart van het internet in Nederland. Het .nl-domein is één van de veiligste domeinen van de wereld en daar zijn we trots op! Onze kennis over online security zetten we ook in om het internet in Nederland veiliger te maken, met initiatieven als SIDN Merkbewaking.

> [Lees meer over wie wij zijn.](#)

Inhoud

1	<u>Inleiding</u>	3
2	<u>Hoe detecteren wij online merkinbreuk?</u>	4
3	<u>Waarom online merkbewaking?</u>	7
4	<u>Domeinnamenbeleid voor mkb'ers: 5 belangrijke adviezen</u>	8
5	<u>Hoe treedt je als mkb'er op tegen merkinbreuk?</u>	9
6	<u>Over MKB Merkbewaking</u>	10
7	<u>Colofon</u>	11





1 Inleiding

Het mkb is steeds vaker doelwit van cybercriminelen. Onlangs nog bleek uit onderzoek van Eurostat dat Nederlandse mkb'ers bovengemiddeld te maken krijgen met cyberaanvallen. 30% van de mkb'ers gaf aan in de afgelopen 12 maanden een incident meegemaakt te hebben, waarmee Nederland na Finland het land met de hoogste frequentie is.

Dat is zorgelijk, zeker nu het mkb sinds COVID-19 steeds afhankelijker is van online.

Gelukkig zijn er steeds meer tools en methoden om je als ondernemer te wapenen tegen cybercrime. Vaak beginnen aanvallen met phishing, namelijk vanaf een domeinnaam die lijkt op die van de ondernemer zelf. Ook gebruiken cybercriminelen logo's en huisstijl om zich als bonafide onderneming voor te doen. Door websites waar dit gebeurt snel op te sporen kan schade voorkomen worden.

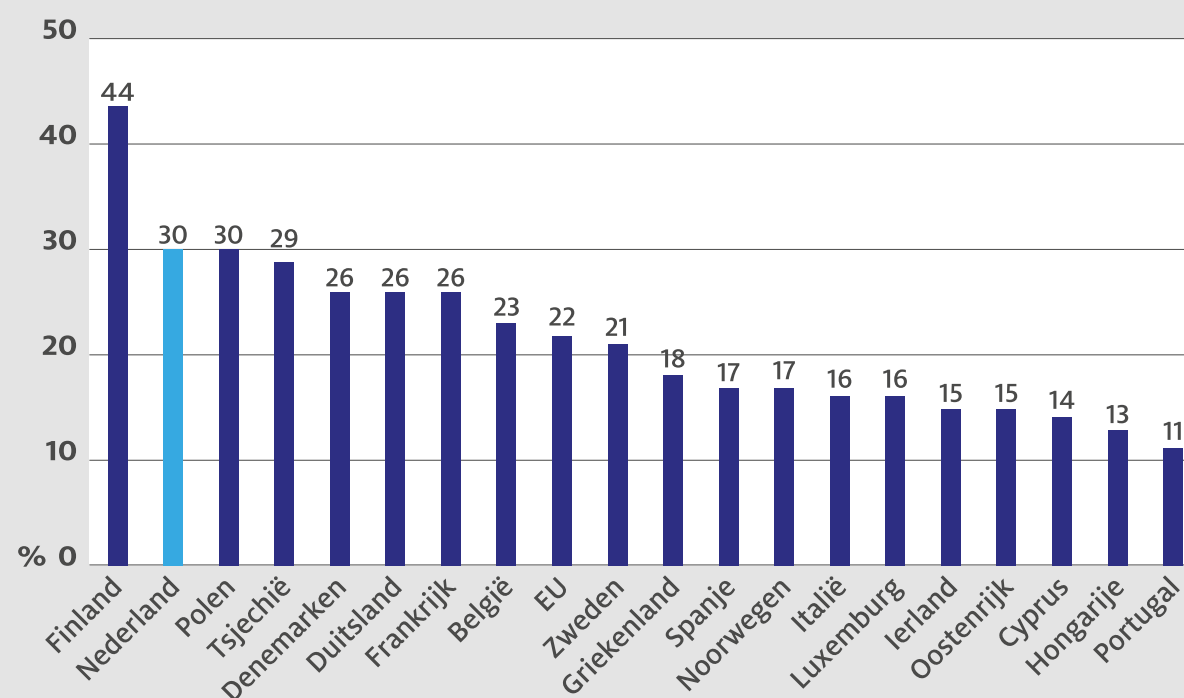
Om deze reden biedt SIDN Merkbewaking voor het mkb aan. Als beheerder van het .nl-domein zetten wij ons dagelijks in om het internet in Nederland veilig en betrouwbaar te houden. Hiervoor ontwikkelen we onder meer diensten die merkhouders helpen hun merk ook online te beschermen. In de afgelopen tien jaar deden wij dit al voor het grootzakelijke segment. Sinds 2022 bieden wij deze dienst via registrars aan mkb'ers.



Wil je meer weten over dit onderwerp?
Kijk dan op <https://mkbmerkbewaking.nl>
of scan de QR code hiernaast.

“Toen ik ontdekte dat mijn logo zonder mijn toestemming elders werd gebruikt, ondernam ik meteen actie, want wie aan mijn merk komt, komt aan mijn bedrijf.”

mkb-ondernemer, gebruiker van MKB Merkbewaking



Afb. 1 | % van de ondernemers die een security-incident meemaakten in de laatste 12 maanden (Bron: Eurostat)



2 Hoe detecteren wij online merkinbreuk?

MKB Merkbewaking maakt gebruik van een rechtstreekse koppeling met de database van alle .nl-domeinnamen, waardoor alle .nl-domeinnamen die (nauw) overeenkomen met een merknaam realtime worden gevonden. Eens in de 24 uur controleert Merkbewaking ook alle registraties onder alle andere topleveldomeinen zoals .com, .de, etc. Het algoritme achter *MKB Merkbewaking* wordt al tien jaar gebruikt in grootzakelijke omgevingen en is door SIDN zelf ontwikkeld.

Naast domeinnamen kijkt *MKB Merkbewaking* binnen de .nl-zone ook naar logo's en beeldmerken. Daarvoor scannen we alle .nl-websites op het gebruik van jouw logo of beeldmerk. Dit geeft je een actueel overzicht van alle .nl-websites met jouw logo erop. Daarnaast biedt SIDN Merkbewaking de mogelijkheid om bij misbruik direct (juridische) actie te ondernemen.

Misbruik van domeinnamen: recente voorbeelden

De gemeente Krimpen aan den IJssel werd begin 2023 voor meer dan 175.000 euro opgelicht.

Een criminele organisatie heeft zich met een vals domein voorgedaan als directielid. Een medewerker werd door hem per mail gevraagd om een aantal rekeningen te betalen. De betalingen gingen naar buitenlandse rekeningen.

Duizenden aanvragers kentekenbewijs gedupeerd

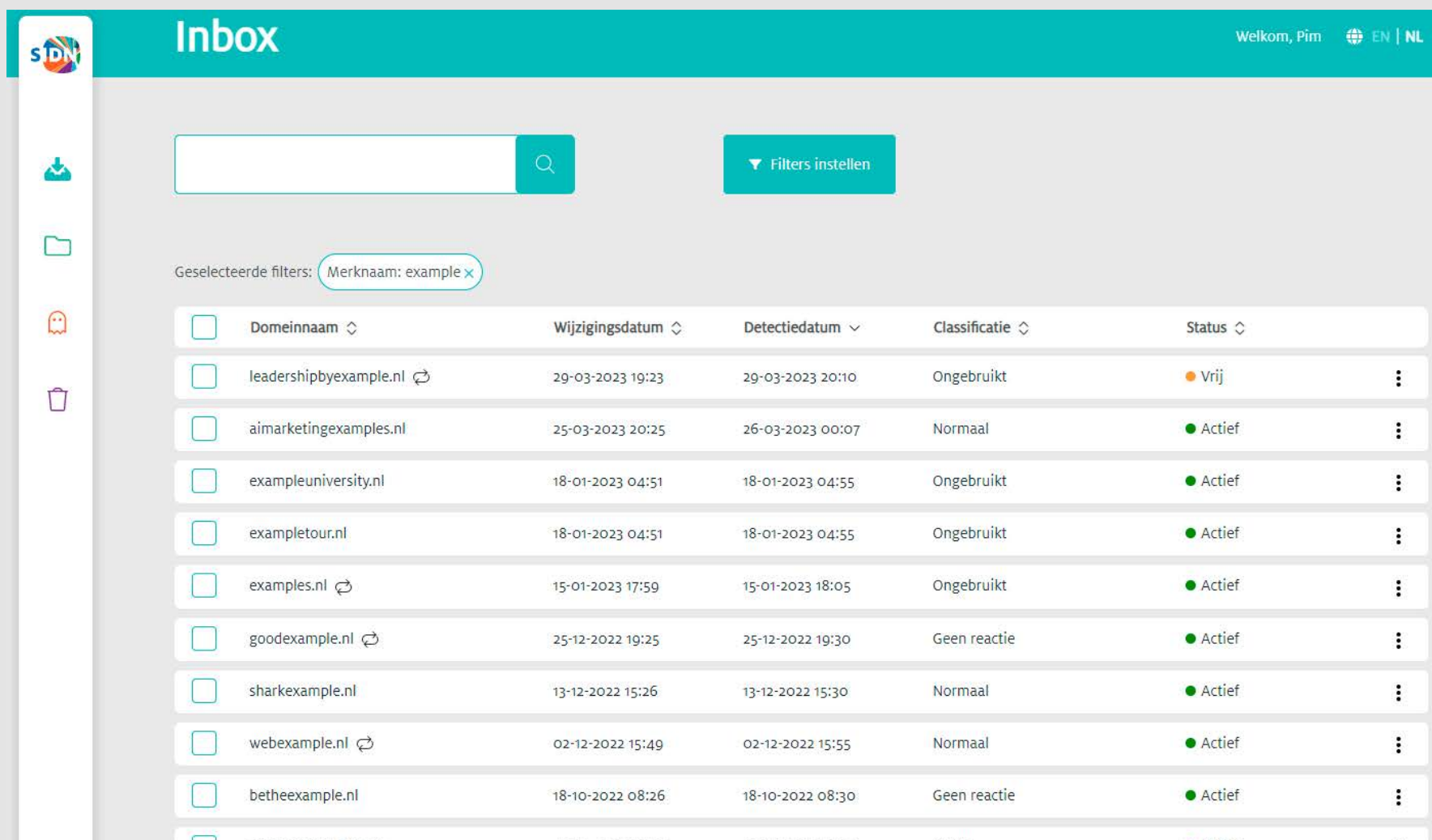
De site rdwservice.nl was uitgevoerd in karakteristiek 'RDW-rood' en liet het kenmerkende veertje zien, dat ook de RDW in haar huisstijl voert. Bezoekers betaalden € 19,95 voor een nieuw kentekenbewijs en... hoorden daarna nooit meer iets. Het overkwam in 2020 duizenden gedupeerden in Nederland.





2

Met MKB Merkbewaking kun je je merk dus beschermen zoals jij dat wilt. In Nederland, maar ook daarbuiten. Resultaten leveren wij wekelijks aan per mail, maar het is ook mogelijk om live toegang te krijgen tot resultaten in een eigen webinterface.



The screenshot shows the SIDN Inbox web interface. The header is teal with the SIDN logo on the left and 'Welkom, Pim' with language options 'EN' and 'NL' on the right. Below the header is a search bar with a magnifying glass icon and a 'Filters instellen' button. The main content area shows a table of search results for the filter 'Merknaam: example'. The table has columns for 'Domeinnaam', 'Wijzigingsdatum', 'Detectiedatum', 'Classificatie', and 'Status'. Each row includes a checkbox, the domain name, and a status indicator (orange dot for 'Vrij', green dot for 'Actief').

☐	Domeinnaam	Wijzigingsdatum	Detectiedatum	Classificatie	Status
☐	leadershipbyexample.nl	29-03-2023 19:23	29-03-2023 20:10	Ongebruikt	Vrij
☐	aimarketingexamples.nl	25-03-2023 20:25	26-03-2023 00:07	Normaal	Actief
☐	exampleuniversity.nl	18-01-2023 04:51	18-01-2023 04:55	Ongebruikt	Actief
☐	exampletour.nl	18-01-2023 04:51	18-01-2023 04:55	Ongebruikt	Actief
☐	examples.nl	15-01-2023 17:59	15-01-2023 18:05	Ongebruikt	Actief
☐	goodexample.nl	25-12-2022 19:25	25-12-2022 19:30	Geen reactie	Actief
☐	sharkexample.nl	13-12-2022 15:26	13-12-2022 15:30	Normaal	Actief
☐	webexample.nl	02-12-2022 15:49	02-12-2022 15:55	Normaal	Actief
☐	betheexample.nl	18-10-2022 08:26	18-10-2022 08:30	Geen reactie	Actief

Afb. 2 | Resultaten van een scan op onze eigen naam.



2

Merkbewaking is effectief

Dat merkbewaking effectief is, blijkt wel uit de resultaten in het grootzakelijke segment die onze oplossing als sinds 2012 gebruiken. Sinds 2012 spoorde deze tool tienduizenden phishingwebsites op. Daardoor vindt phishing steeds minder vanaf Nederlandse websites en met gebruik van grote Nederlandse merken plaats.

	2016	2022	Toename %
Aantal website die overeenkomen met top-50 merken	30.682	24.805	-19
Aantal websites	675	1079	60
Aantal top-50 merken beschermd door Merkbewaking	10	42	600

Keerzijde van die effectiviteit is dat cybercriminelen zich steeds meer gingen richten op minder bekende merken en bedrijven in het mkb. Ook werken cybercriminelen nu vaker vanuit sites en domeinnamen buiten Nederland en de EU. Zo is .ml, het domein van Mali, erg populair voor phishing in Nederland door de grote gelijkenis met .nl. In andere woorden: door betere beveiliging gaan criminelen op zoek naar makkelijkere doelwitten.

Meer weten over het bestrijden van domeinnaammisbruik?

Lees ons artikel '3 redenen waarom het monitoren van domeinnamen een goed idee is'.



3 Waarom online merkbewaking?

Het gebruik van domeinnamen om je voor te doen als een bonafide organisatie is een vorm van 'typosquatting'. Typosquatting is een vorm van internetmisbruik, waarbij sterk op de originele naam gelijkende domeinnamen geregistreerd worden. Het doel is dat de beoogde slachtoffers zich vergissen bij het lezen van een mail- of webadres en denken met het echte bedrijf van doen te hebben. In de meest onschuldige variant wordt deze naar sites met reclame geleid of naar een concurrerende website, maar vaak heeft de typosquatsite een criminele intentie. Bijvoorbeeld het sturen van valse facturen of toegang tot vertrouwelijke netwerken verkrijgen.

Dat versturen van valse facturen staat ook wel bekend als CEO-fraude. Deze naam is afgeleid van de werkwijze waarbij cybercriminelen een valse e-mail sturen uit naam van de CEO, een directeur of manager van de organisatie. Zij vragen een financieel- of administratiemedewerker dan bijvoorbeeld om met spoed een groot bedrag over te maken, meestal naar het buitenland.

Als de medewerker het niet vertrouwt, volgt er vaak een telefoongesprek. Hiervoor roepen de criminelen een niet-bestaande derde partij in het leven, een zogenaamd advocatenkantoor. Deze telefoontjes lijken zo betrouwbaar dat de medewerker, volkomen te goeder trouw, het gevraagde bedrag overmaakt. Het grootste geval van CEO-fraude in Nederland leidde tot een schade van € 19,4 miljoen voor bioscoopketen Pathé. Bedragen van meer dan € 100.000,- komen regelmatig voor.

Om zich als CEO van een bedrijf voor te doen kunnen doen, kunnen cybercriminelen een gelijkende domeinnaam registreren en daar een mailadres bij aanmaken. Bijvoorbeeld: <naamdirecteur>@rabobank.nl (nul in plaats van o). Een simpele methode die snel opgezet kan worden. Een omslachtiger methode is het mailadres van de CEO technisch te 'spoofen'. Gelukkig zijn er mailbeveiligingsstandaarden beschikbaar die dit tegengaan: DKIM, SPF en DMARC. Om de beveiliging van je mailverkeer nog verder te verhogen raden we nadrukkelijk aan om deze standaarden te gebruiken in combinatie met DNSSEC, een beveiligingssysteem voor het DNS. Je leest er meer over op <https://www.sidn.nl/cybersecurity/moderne-internetstandaarden>.

Maar typosquatting kan ook gebruikt worden om een systeem te gijzelen. De mail van de 'CEO' bevat dan een link of bijlage met malware die de computer van de ontvanger overneemt, waarna de cybercrimineel bijvoorbeeld ransomware kan installeren. De schade hiervan kan ook zeer snel oplopen. Reden genoeg dus om actief op te treden tegen online misbruik van je merknaam.

Merkbewaking is daarnaast ook bruikbaar voor het detecteren van legitiem, niet-malafide gebruik. Legitiem gebruik van het logo of beeldmerk is gebruik dat misschien ongewenst, maar niet illegaal is. Zo biedt de tool ook de mogelijkheid om te kijken hoe bedrijfsonderdelen, partners, klanten, leveranciers en franchisenemers omgaan met het beeldmerk, of waar diensten en producten van het bedrijf online geleverd worden. De tool wordt om die reden op dit moment al gebruikt door diverse keurmerken.



4 Domeinnamenbeleid voor mkb'ers: 5 belangrijke adviezen

1. Zet een domeinnaam altijd op naam van de organisatie

Een veel gemaakte fout door bedrijven is een campagne starten of mail versturen vanaf een domein dat niet op de naam van het bedrijf staat. Daardoor kan bij klanten twijfel ontstaan over de afzender. Bovendien kunnen er problemen ontstaan wanneer de provider van je website zijn bedrijf beëindigt of je van leverancier wilt wisselen.

2. Zorg voor een bekend domeinnaamregistratiepunt dat altijd bereikbaar is

Zorg dat al je medewerkers weten wat je domeinnaamregistratiebeleid is en bij welke leverancier je je domeinnamen registreert. Maak de registratieprocedure niet te ingewikkeld is: dat moedigt ontwijkend gedrag juist aan.

3. Voldoen aan veiligheidsstandaarden

Veel domeinnamen worden als verdacht bestempeld, omdat ze in technische zin niet voldoen aan de voor het doel gebruikelijke standaarden (vb. geen SSL-certificaat). Zorg er daarom voor dat interne en externe betrokkenen aan de security- en privacy-eisen voldoen. Een tip: kijk op internet.nl en test hoe veilig jouw site is.

4. Detecteer valse domeinen in een vroeg stadium

Om te profiteren van een te kwader trouw geregistreerde domeinnaam is het voor kwaadwillenden noodzakelijk dit zo lang mogelijk in de lucht te houden. Een monitoringoplossing zoals MKB Merkbewaking kan een mogelijke malafide .nl-domeinnaam al direct bij registratie opsporen en dus vóór de site live is.

5. Denk ook goed na over het opheffen van domeinnamen

Oude domeinnamen van organisaties zijn geliefd bij cybercriminelen, omdat ze vertrouwd worden. Na opheffing worden ze vaak opgepikt en gebruikt om spam te versturen of zich voor te doen als medewerker van de organisatie. Denk dus ook goed na, voordat je een domeinnaam opheft.

Wil je meer praktische tips over het vastleggen van domeinnamen bij je merk? Lees ons artikel: [‘Zo bescherm je je merk online’ op sidn.nl](#)





5 Hoe treed je als mkb'er op tegen merkinbreuk?

Veel bedrijven zijn zich er onvoldoende van bewust dat ze ook zonder tussenkomst van de rechter tegen online merkinbreuk kunnen optreden. Dat is meestal goedkoper, makkelijker en sneller dan naar de rechter. Er zijn drie opties:

1. Voor domeinnamen eindigend op .nl is de geschillenregeling te vinden op sidn.nl.
2. Voor andere landen is een andere organisatie (de zgn. registry) verantwoordelijk. Een lijst van registries per vind je op [IANA.org](https://iana.org). Kijk op hun site voor meer informatie.
3. De regeling voor .com en andere niet-landgebonden extensies vind je op [WIPO.int](https://wipo.int) en op icann.org.

Hieronder staat kort uitgelegd wat je in welke situatie moet doen.

	.nl	.com (en andere niet-landgebonden extensies)
Inbreuk op jouw merk- of handelsnaam.	• Start een geschillenregeling voor .nl-domeinnamen (kijk hier voor meer informatie). • Stap naar de recht (duurder).	Vul een Uniform Domain Name Dispute Resolution formulier in.
Onrechtmatige content op een site (bijv. malafide webshop met nepproduct).	Vraag de provider van die site om deze offline te halen (Notice-and-Take-Down).	Vraag de provider van die site om deze offline te halen (Notice-and-Take-Down).
Klacht over een provider die ook de domeinnamen registreert.	Dien een klacht in bij SIDN via deze link .	Gebruik dit formulier om een klacht in te dienen (ICANN.org).



6 Over MKB Merkbewaking

MKB Merkbewaking is een monitoringsdienst die je helpt bij het bestrijden van cybercrime. Met deze service spoor je effectief typosquatting en CEO-fraude op. Typosquatting is het registreren van web- of mail-adressen die lijken op je merk om met gerichte aanvallen (persoons) gegevens of geld te ontvreemden. Bij CEO-fraude doen cybercriminelen zich met nepmails voor als CEO, directeur of manager en vragen medewerkers om met spoed een groot bedrag over te maken. Vaak met grote schade voor het bedrijf tot gevolg.

Daarnaast draagt MKB Merkbewaking bij aan het versterken van je merkwaarde. Het spoort uit beeld geraakte websites en domeinnamen op en helpt brandmanagers te zien wie hun merk gebruikt en of dit correct gebeurt. Denk bijvoorbeeld aan gebruik door retailers, partners of tussenpersonen. Ook voorkom je dat concurrenten je naam op ongeoorloofde wijze gebruiken.





Colofon

Dit is een verslag van een onderzoek dat is uitgevoerd door SIDN.

Aan dit verslag werkten mee:

Michiel Henneke – Marketingmanager

Pim Pastoors – Productmanager New business Marketing en Sales

Heb je vragen over het onderzoek, mail dan naar merkbewaking@sidn.nl.

© SIDN

Teksten en cijfers uit dit whitepaper mag je overnemen, maar wij willen dan wel graag als bron vermeld worden. Ook worden wij graag vooraf geïnformeerd via communicatie@sidn.nl.

Meld je aan voor onze nieuwsbrief

www.sidn.nl/nieuwsbrief

SIDN

Postbus 5022

6802 EA Arnhem

Meander 501

6825 MD Arnhem

T +31 (0)26 352 55 00

www.sidn.nl