Consultatie wetsvoorstel Cyberbeveiligingswet

Stichting BREIN (hierna: "BREIN") verzorgt de collectieve bescherming van auteurs- en naburig recht voor makers, uitvoerende kunstenaars en de creatieve media-industrie zoals producenten, uitgevers, omroepen, distributeurs en platforms. Aangesloten bij BREIN zijn rond de dertig branche- en collectieve beheersorganisaties en hun leden, tezamen enkele duizenden bedrijven en tienduizenden makers met betrekking tot muziek, films, series, boeken, geschriften, beeld en games. BREIN detecteert en bestrijdt grootschalige auteursrechtinbreuk en -misbruik namens haar aangeslotenen, verzorgt voorlichting en stimuleert legaal gebruik.

BREIN is ruim 25 jaar actief. Al sinds de opkomst van het internet werkt BREIN aan een raamwerk van rechtspraak waaruit de verantwoordelijkheden en zorgplichten van internet tussenpersonen blijkt. Waar BREIN lange tijd een van de weinige partijen was die civielrechtelijk online handhaving als focus had, juicht BREIN toe dat er steeds meer partijen zijn die zich realiseren dat online handhaving essentieel is om een veilig online klimaat te creëren. Ook is BREIN verheugd dat er steeds meer codificatie plaatsvindt van spelregels voor partijen die online actief zijn.

De NIS2-richtlijn en Cyberbeveiligingswet zien op een breed palet aan onderwerpen. Voor de praktijk van BREIN bestaande uit de online handhaving tegen inbreuken op auteursrechten en naburige rechten is vooral artikel 28 van de NIS2-richtlijn relevant. Deze bijdrage van Stichting BREIN ziet op de implementatie van dit artikel.

Het bieden van toegang tot betrouwbare registrantgegevens ("WHOIS-gegevens") is essentieel voor het bestrijden van illegale en schadelijke online-inhoud, waaronder inhoud die inbreuk maakt op auteursrechten. In een studie van de Europese Commissie van 2022 over DNS-misbruik werd de verificatie van WHOIS-gegevens genoemd als een van de belangrijkste aanbevelingen om DNS-misbruik te voorkomen, op te sporen en te beperken. [1] Stichting BREIN wil benadrukken dat verstrekte WHOIS-gegevens nauwkeurig en geverifieerd moeten zijn en betrekking moeten hebben op de daadwerkelijke gebruiker van de domeinnaam en niet alleen op een aanbieder van privacy- of proxydiensten.

Met het oog op de implementatie van de NIS2-richtlijn willen we graag de volgende prioriteiten benadrukken om ervoor te zorgen dat artikel 28 juist wordt geïmplementeerd en de toegankelijkheid en nauwkeurigheid van WHOIS-gegevens aanzienlijk worden verbeterd.

legitieme toegangvragende partijen en gegevens

Overweging 110 van de NIS2-Richtlijn omschrijft ‘legitieme toegangvragende partijen’ van WHOIS-gegevens als bedoeld in artikel 28, lid 5, als ‘elke natuurlijke of rechtspersoon die een verzoek

[1] ‘Study on Domain Name System (DNS) Abuse’, Europese Commissie 2021, https://op.europa.eu/s/zLB2

indient krachtens het Unie- of nationale recht'. In de MvT bij het wetsvoorstel is verduidelijkt dat 'legitieme toegangvragende partijen' niet alleen worden gedefinieerd als overheidsinstanties maar ook als elke natuurlijke of rechtspersoon die een verzoek om toegang tot WHOIS-gegevens indient. Wellicht kan dit ook in de begripsbepalingen onder artikel 1 van de wet zelf worden opgenomen. Dit is in overeenstemming met de aanbeveling van de Europese Commissie betreffende de bestrijding van namaak, waarin entiteiten die domeinnaamregistratiediensten in de EU aanbieden, worden aangemoedigd om alle natuurlijke of rechtspersonen die een verzoek indienen voor een recht op informatie op grond van Richtlijn 2004/48/EG betreffende de handhaving van intellectuele-eigendomsrechten, te erkennen als legitieme toegangvragende partijen.[2]

Noodzakelijke informatie database

In het tweede lid van artikel 50 van het wetsvoorstel (de implementatie van artikel 28 lid 2 NIS2-richtlijn) is opgenomen dat de database 'de naam, het e-mailadres en het telefoonnummer van de registrant' moet bevatten. Volgens artikel 28 lid 2 NIS2-richtlijn zijn deze gegevens noodzakelijk 'om de houders van de domeinnamen en de contactpunten die de domeinnamen onder de topleveldomeinnamen beheren, te identificeren en te contacteren.' Naar de mening van BREIN is het opnemen in de WHOIS-database van enkel de naam, e-mailadres en telefoonnummer van de registrant onvoldoende om voornoemd doel te bereiken. Natuurlijke personen zijn in de regel alleen tot een identificeerbaar persoon te herleiden indien naast de naam ook het adres van deze persoon bekend is. Indien de betreffende registrant niet reageert op verzoeken via e-mail of telefoon kan een natuurlijk persoon zonder bekend adres niet effectief (zonodig in rechte) worden aangesproken. BREIN stelt daarom voor om in artikel 2 lid 2 onder c naast de naam, het e-mailadres en het telefoonnummer, ook het adres van de registrant op te nemen, indien die registrant een natuurlijk persoon is. Dit is ook in lijn met het 'recht op informatie' op grond van artikel 8 lid 2 van Richtlijn 2004/48/EG betreffende de handhaving van intellectuele-eigendomsrechten.

Gebruik van proxy-/privacydiensten

In een studie uit 2021 van het EU-Bureau voor de Intellectuele Eigendom (EUIPO) wordt opgemerkt dat een significant percentage van de domeinnamen die worden gebruikt voor illegale of schadelijke internetactiviteiten worden geregistreerd via privacy- of proxydiensten[3] en dat sinds de inwerkingtreding van de AVG de beweegredenen voor het legitieme gebruik van privacy- of proxydiensten in twijfel worden getrokken.[4]

[2] Aanbeveling Europese Commissie 2024/915, par. 15, https://op.europa.eu/s/zLB3.
[3] 'Domain Names: Discussion Paper', EUIPO maart 2021, p.9 https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Discussion_Paper_on_Domain_Names/2021_Discussion_Paper_on_Domain_Names_FullR_en.pdf.
[4] Ibid., p. 20.

Bij de nationale omzetting van de NIS2 -richtlijn moet daarom rekening worden gehouden met de populariteit van proxy- of privacydiensten onder degenen die illegale en schadelijke online activiteiten uitvoeren. Wanneer een legitiem verzoek om toegang wordt gedaan, moeten de onderliggende gegevens van de werkelijke klant/de werkelijke gebruiker van de domeinnaam worden onthuld en dus niet alleen de gegevens van de aanbieder van de privacy- of proxydienst als bij het registratieproces gebruik is gemaakt van een dergelijke privacy- of proxydienst.

We bevelen daarom aan om aan artikel 51 lid 1 van de Cyberbeveiligingswet expliciet de volgende formulering toe te voegen (of een formulering van gelijke strekking): "*Deze specifieke gegevens betreffen de gegevens van de uiteindelijke gebruiker van de domeinnaam. Het is onvoldoende om de gegevens te verstrekken van de aanbieder van de privacy- of proxy-registratiedienst die mogelijk bij het registratieproces van de domeinnaam is gebruikt.*"

In dit verband moet de omzetting van de verplichtingen van artikel 28 om de juistheid van WHOIS-gegevens te controleren duidelijk van toepassing zijn op aanbieders van privacy- en proxy-diensten en wederverkopers van domeinnamen, alsmede op registrars en registers voor topleveldomeinen. Dit is in lijn met het beleid van bijvoorbeeld SIDN, het register voor .nl domeinnamen, die sinds 1 oktober 2023 niet langer toestaat dat een .nl-domeinnaam op naam van een derde partij (zoals privacy- en proxydienstverleners, maar ook registrars en resellers van .nl domeinnamen) geregistreerd wordt.[5]

Reverse WHOIS

Cybercriminelen registreren vaak meer, soms zelfs duizenden domeinnamen in korte tijd. Wij bevelen aan om in de wet op te nemen dat legitieme toegangvragende partijen een volledige lijst kunnen verkrijgen van alle domeinnamen die zijn geregistreerd onder dezelfde registrant (“reverse WHOIS lookup”) wanneer illegale activiteiten zijn geconstateerd.

Thick WHOIS

Het enige register voor .com en .net topleveldomeinnamen is goed voor meer dan de helft van alle geregistreerde domeinnamen wereldwijd en heeft contracten met meer dan 2.000 registrars over de hele wereld. Overheidsinstanties en legitieme toegangvragende partijen moeten momenteel de relevante registrar opsporen om WHOIS-gegevens op te vragen. Het moeizame proces dat dit met zich meebrengt, en de realiteit dat de registrar zich in een land kan bevinden dat niet meewerkt aan dergelijke verzoeken, ondermijnt het doel van het vergroten van de cyberveiligheid en dient in plaats daarvan als dekmantel en bescherming voor illegale actoren. Het is daarom essentieel dat dit register, evenals alle andere registers voor topleveldomeinen, een volledige, nauwkeurige en onafhankelijke database van WHOIS-gegevens bijhouden voor alle domeinnamen die zij beheren (aangeduid als "Thick WHOIS") en deze gegevens moeten de

[5] Zie https://www.sidn.nl/nieuws-en-blogs/vanaf-1-oktober-geldt-een-verbod-op-privacy-en-proxyservices-onder-nl

gegevens van de uiteindelijke gebruiker van de domeinnaam bevatten en niet alleen de gegevens van een aanbieder van privacy- of proxydiensten die mogelijk zijn gebruikt in het registratieproces (zie hierboven). SIDN is een voorbeeld van een topleveldomein register dat het Thick WHOIS model hanteert. Dit zorgt ervoor dat handhavingsinstanties en andere legitieme toegangvragende partijen zich kunnen richten tot één gecentraliseerde partij waar volledige en nauwkeurige gegevens kunnen worden opgevraagd over alle domeinnamen die door het topleveldomein register worden beheerd.

* * *