Bundesverband Musikindustrie e.V., Linienstr. 152, 10115 Berlin

Bundesministerium des Inneren und für Heimat
Abteilung CI – Cyber- und Informationssicherheit
Alt-Moabit 140
10557 Berlin

nur per E-Mail: *ci@bmi.bund.de; nis2@bmi.bund.de*

Berlin, den 28. Mai 2024

Stellungnahme des Bundesverband Musikindustrie e.V. (BVMI) zum „Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ des Bundesministeriums des Innern und für Heimat (BMI)

Umsetzung der NIS2-Richtlinie: Erfüllung des in Artikel 28 festgelegten Ziels des öffentlichen Zugangs zu zuverlässigen WHOIS-Informationen

Der Bundesverband Musikindustrie (BVMI) vertritt die Interessen von mehr als 200 Tonträgerherstellern und Musikunternehmen, die mehr als 80 Prozent des deutschen Musikmarkts repräsentieren. Der Verband setzt sich für die Anliegen der Musikindustrie in der deutschen und europäischen Politik ein und dient der Öffentlichkeit als zentraler Ansprechpartner zur Musikbranche. Neben der Ermittlung und Veröffentlichung von Marktstatistiken sowie der Etablierung von Branchenstrukturen wie der B-to-B-Plattform PHONONET gehören branchennahe Dienstleistungen zum Portfolio des BVMI. Seit 1975 verleiht er die GOLD- und PLATIN-, seit 2014 auch die DIAMOND-AWARDS an die erfolgreichsten Künstler in Deutschland. Seit 1977 werden die Offiziellen Deutschen Charts im Auftrag des BVMI erhoben. Zur Orientierung der Verbraucher bei der legalen Nutzung von Musik im Internet hat der Verband 2013 die Initiative PLAYFAIR ins Leben gerufen.

Der BVMI begrüßt die Verabschiedung der überarbeiteten Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS2-Richtlinie), insbesondere die Bestimmungen über Domänennamen- und Registrierungsdienste in Artikel 28 und den Erwägungsgründen 109 bis 112. Der Zugang zu zuverlässigen Registrierungsdaten ("WHOIS-Daten") ist für die Bekämpfung illegaler und schädlicher Online-Inhalte, einschließlich urheberrechtsverletzender Inhalte, und für den

Schutz der Gesundheit und Sicherheit der Bürger von wesentlicher Bedeutung. Die Umsetzung von Artikel 28 findet sich in den §§ 51-53 des „Entwurfs eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“.

Insofern schließt sich der BVMI auch der Position der Motion Picture Association (MPA) an.

In der Studie der Europäischen Kommission über DNS-Missbrauch aus dem Jahr 2022 wurde die Überprüfung von WHOIS-Daten als eine der wichtigsten Empfehlungen zur Verhinderung, Aufdeckung und Eindämmung von DNS-Missbrauch genannt. Auch die Europäische Kommission hat kürzlich in der Empfehlung zur Bekämpfung von Produkt- und Markenpiraterie aus dem Jahr 2024 anerkannt, dass "die Richtigkeit und Vollständigkeit der Registrierungsdaten von Domänennamen auch eine zentrale Rolle bei der Durchsetzung von Rechten des geistigen Eigentums spielen kann" (eigene Übersetzung). Sie betonte ferner, dass die bereitgestellten Registrierungsdaten korrekt und verifiziert sein und sich auf den tatsächlichen Nutzer des Domänennamens beziehen müssen, und nicht einfach auf einen Anbieter von Datenschutz- oder Proxy-Diensten.

Wir begrüßen den Gesetzesentwurf des BMI, der eine weitgehend wortgetreue Umsetzung von Artikel 28 vornimmt. Wir möchten jedoch die folgenden Prioritäten hervorheben, um eine solide Umsetzung zu gewährleisten und die Zugänglichkeit und Genauigkeit der WHOIS-Daten weitgehend zu verbessern:

- **Berechtigte Zugangsnachfrager und Daten**: In Erwägungsgrund 110 der NIS2 wird der „berechtigte Zugangsnachfrager“ auf Zugang zu WHOIS-Daten gemäß Artikel 28 Absatz 5 als „jede natürliche oder juristische Person zu verstehen, die einen Antrag gemäß des Unionsrechts oder des nationalen Rechts stellt" definieren.

  Das deutsche Umsetzungsgesetz sollte daher den Begriff "berechtigte Zugangsnachfrager" ausdrücklich definieren und klarstellen, dass dazu nicht nur staatliche Stellen, wie z. B. Strafverfolgungsbehörden, gehören, sondern auch **jede natürliche oder juristische Person, die einen Antrag auf Zugang zu WHOIS-Daten stellt**, **um die Rechtswidrigkeit zu untersuchen**, einschließlich, aber nicht beschränkt auf die Begründung, Ausübung oder Verteidigung von Rechtsansprüchen in den Bereichen Cybersicherheit, geistiges Eigentum, Verbraucherschutz oder andere Rechtsansprüche.

  Dies steht im Einklang mit der kürzlich veröffentlichten Empfehlung der Europäischen Kommission zur Bekämpfung von Produkt- und Markenpiraterie, in der Unternehmen, die in

der EU Registrierungsdienste für Domänennamen anbieten, aufgefordert werden, natürliche oder juristische Personen, die einen Antrag auf Auskunftserteilung gemäß der Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums (IPRED) stellen, als berechtigte Zugangsnachfrager anzuerkennen.[1]

In der Tat arbeiten die Strafverfolgungsbehörden häufig mit unabhängigen Forschern und Nichtregierungsorganisationen zusammen, um illegale Online-Aktivitäten zu verfolgen und zu bekämpfen.[2]

Wir schlagen daher folgende Formulierung für die Umsetzung in deutsches Recht vor:

> *"Zu den berechtigten Zugangsnachfragern gehört jede natürliche oder juristische Person, die einen Antrag zur Feststellung, Ausübung oder Verteidigung von straf-, zivil- oder sonstigen Rechtsansprüchen nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland stellt.*"

Darüber hinaus muss der Zugang zu den WHOIS-Daten gemäß Erwägungsgrund 112 kostenlos sein, und diese Daten müssen auf Antrag des berechtigten Zugangsnachfragers ohne unangemessene Verzögerung zur Verfügung gestellt werden.

- **Bekämpfung der Nutzung von Proxy-/Privacy-Diensten:** In einer Studie des EU-Amtes für geistiges Eigentum (EUIPO) aus dem Jahr 2021 wurde festgestellt, dass "ein erheblicher Prozentsatz der Domänennamen, die zur Durchführung illegaler oder schädlicher Internetaktivitäten verwendet werden, über Datenschutz- oder Proxy-Dienste registriert werden" und dass seit dem Inkrafttreten der Datenschutz-Grundverordnung die Begründung für die rechtmäßige Nutzung von Datenschutz- oder Proxy-Diensten "in Frage gestellt wurde" (eigene Übersetzung). [3]

  Die nationale Umsetzung der NIS2-Richtlinie muss daher die Beliebtheit von Proxy- oder Privacy-Diensten bei denjenigen berücksichtigen, die illegale und schädliche Aktivitäten online durchführen. Wenn ein berechtigter Zugangsantrag gestellt wird, müssen die

[1] Siehe Empfehlung über Maßnahmen zur Bekämpfung von Nachahmungen und zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums, Ziffer 15.
[2] Siehe zum Beispiel das Europäische Zentrum zur Bekämpfung der Cyberkriminalität, das "darauf abzielt, Akteure des öffentlichen und privaten Sektors einzubinden, deren Fähigkeiten, Ressourcen und Reichweite neben den Bemühungen der Strafverfolgungsbehörden benötigt werden, um ein sichereres digitales Umfeld zu schaffen." https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[3] EUIPO "Domain Names: Diskussionspapier" März 2021 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

zugrundeliegenden Daten des tatsächlichen Kunden/begünstigten Nutzers des Domänennamens offengelegt werden und nicht nur die Daten des Anbieters des Datenschutz- oder Proxy-Dienstes, wenn ein solcher Datenschutz- oder Proxy-Dienst bei der Registrierung verwendet wurde.

Wir empfehlen daher, dass der deutsche Gesetzesentwurf bei der Umsetzung von Artikel 28 ausdrücklich die folgende Formulierung enthält:

> *"Bei der Bereitstellung von Daten als Antwort auf rechtmäßige Zugangsanträge müssen TLD-Namen-Register und die Stellen, die Domänennamen-Registrierungsdienste anbieten, die Daten des wirtschaftlichen Nutzers des Domänennamens bereitstellen und dürfen stattdessen nicht die Daten des Anbieters von Datenschutz- oder Proxy-Registrierungsdiensten bereitstellen, die bei der Registrierung des Domänennamens verwendet worden sein könnten."*

In dieser Hinsicht sollte die Umsetzung der in Artikel 28 festgelegten Verpflichtung zur Überprüfung der Richtigkeit der WHOIS-Daten eindeutig für Anbieter von Datenschutz- und Proxy-Diensten und Wiederverkäufer von Domänennamen sowie für Registrierungsstellen und TLD-Register gelten. Dies steht im Einklang mit Artikel 6 (22), der ausdrücklich Anbieter von Datenschutz- und Proxy-Diensten sowie Wiederverkäufer von Domänennamen als Beispiele für "Einrichtung, die Domänennamen-Registrierungsdienste erbringt", aufführt.

- **DNS-Missbrauch in großem Umfang angehen und verhindern:** Cyberkriminelle registrieren oft mehrere, manchmal sogar Tausende von Domänennamen in einem kurzen Zeitraum. Dies ist insbesondere der Fall, wenn es um Phishing, die Verbreitung von Malware und die Verbreitung von urheberrechtsverletzenden Inhalten geht. Die Sicherstellung, dass ein rechtmäßiger Zugangssuchender in der Lage ist, eine Liste aller Domänennamen zu erhalten, die unter denselben Registrierungsdaten registriert sind (umgekehrte WHOIS-Abfrage), ist von entscheidender Bedeutung, wenn ausgeklügelte und verstreute illegale Aktivitäten in einem solchen Umfang vermutet werden.

  Wir empfehlen daher, Artikel 28 dahingehend umzusetzen, dass

  > *"wenn ein Domänenname mit missbräuchlichen oder illegalen Aktivitäten in Verbindung gebracht wird, wie dies von einem rechtmäßigen Antragsteller behauptet wird, die TLD-Register und Einrichtungen, die Dienste zur Registrierung von Domänennamen anbieten, dem rechtmäßigen Antragsteller auf Anfrage eine*

Liste aller Domänennamen zur Verfügung stellen müssen, die sie unter denselben Registrierungsdaten verwalten oder registriert haben."

- **Juristische Personen:** Die WHOIS-Daten von juristischen Personen (mindestens Name und Telefonnummer sowie E-Mail-Adresse der Kontaktperson) müssen gemäß Artikel 28 Absatz 4 unter Bezugnahme auf Erwägungsgrund 112 öffentlich zugänglich gemacht werden.

- **Verifizierung:** Die Verfahren zur Überprüfung der WHOIS-Daten sollten solide sein und laufend aktualisiert werden, um Verbesserungen der Technologien und Prozesse zu berücksichtigen. Wie in Erwägungsgrund 111 dargelegt, sollten diese Verfahren " unrichtige Registrierungsdaten zu verhindern bzw. zu berichtigen" und "die in dem Wirtschaftszweig angewandten bewährten Verfahren und, soweit möglich, die Fortschritte im Bereich der elektronischen Identifizierung berücksichtigt werden" und sowohl "Ex-ante-Kontrollen zum Zeitpunkt der Registrierung und Ex-post-Kontrollen nach der Registrierung" umfassen.

  Auch wenn die TLD-Register nicht in der Lage sind, die WHOIS-Daten zum Zeitpunkt der Registrierung zu überprüfen, da die anfängliche Erfassung der Daten in der Regel von Registrierstellen und/oder Datenschutz-/Proxy-Diensten vorgenommen wird, können sie durchaus Ex-post-Verfahren zur Überprüfung der WHOIS-Daten durchführen.

  Wir empfehlen, dass die deutsche Umsetzung Ex-post-Überprüfungsverfahren wie diese für TLD-Namensregister verbindlich macht.

- **Thick WHOIS**: Das einzige TLD-Register für .com und .net ist für mehr als die Hälfte aller weltweit registrierten Domänennamen verantwortlich und hat Verträge mit mehr als 2.000 Registrierstellen in der ganzen Welt. Regierungsbehörden und andere berechtigte Zugangsnachfrager sind derzeit gezwungen, die zuständige Registrierstelle ausfindig zu machen, um eine WHOIS-Datenanfrage zu stellen. Der damit verbundene mühsame Prozess und die Tatsache, dass sich die Registrierungsstelle in einem Land befinden kann, das in Bezug auf solche Anfragen nicht kooperativ ist, untergräbt das Ziel der Erhöhung der Cybersicherheit völlig und dient stattdessen dazu, illegalen Akteuren Deckung und Schutz zu bieten.

Es ist von wesentlicher Bedeutung, dass dieses Register sowie alle anderen TLD-Register eine vollständige, genaue und unabhängige Datenbank mit WHOIS-Daten für **alle** von ihnen verwalteten Domänennamen unterhalten (als "Thick WHOIS" bezeichnet), und diese Daten **müssen** die Daten des wirtschaftlichen Nutzers des Domänennamens **enthalten** und nicht einfach die Daten eines

Anbieters von Datenschutz- oder Proxydiensten, der möglicherweise bei der Registrierung verwendet wurde (siehe oben). Mit dieser wichtigen Anforderung wird sichergestellt, dass Strafverfolgungsbehörden und andere berechtigte Zugangsnachfrager eine zentrale und einzige Quelle haben, von der sie vollständige und genaue Daten über jeden vom TLD-Register verwalteten Domänennamen abrufen können.

René Houareau
Geschäftsführer Recht & Politik