

Anti-Abuse-Richtlinie

Die folgende Richtlinie („HAMBURG Anti-Abuse-Richtlinie“) wird gemäß dem Vertrag zwischen der Registry und den Registraren (Registry-Registrar Agreement, „RRA“) eingeführt und tritt nach einer Frist von dreißig Tagen nach Bekanntgabe durch die Hamburg Top-Level-Domain GmbH („Registry“) gegenüber den Registraren in Kraft. Die missbräuchliche Verwendung von .HAMBURG-Domains wird nicht toleriert.

Die Richtlinie behandelt die allgemeinen Aspekte der Verhinderung missbräuchlicher Verwendung, akzeptabler Nutzung und rascher Erkennung und Verfolgung (rascher Takedown); sie gilt für Registrare und Registranten von .HAMBURG-Domains und definiert das Vorgehen der Registry bei gemeldeten Missbrauchsfällen. Die Richtlinie ersetzt die Uniform Dispute Resolution Policy (UDRP) oder Uniform Rapid Suspension (URS) oder andere Streitschlichtungsverfahren nicht.

Ziel der Registry ist es, dass keine Domain in der gTLD .HAMBURG auf eine Weise genutzt wird (akzeptable Nutzung), die die Rechte Dritter verletzt oder gegen geltendes Recht, staatliche Vorschriften oder Anforderungen verstößt, oder zu Zwecken unrechtmäßiger oder betrügerischer Handlungen einschließlich Spam- oder Phishing-Aktivitäten eingesetzt wird. Nichteinhaltung der Bestimmungen oben kann zur Aussetzung oder Aufhebung der Eintragung des Domains durch die Registry führen.

Die Registry wird zusammen mit dem Registry-Service-Provider die erforderlichen betrieblichen und technischen Schritte zur Förderung der WHOIS-Datengenauigkeit unternehmen, Domainmissbrauch einschränken, veraltete und ungenaue Daten entfernen und andere Sicherheitsmaßnahmen zur Sicherstellung der Integrität des Namensraums .HAMBURG ergreifen. Zu den speziellen Maßnahmen gehört unter anderem eine Anti-Abuse-Richtlinie, die Missbrauch deutlich definiert, Informationen über eine Kontaktstelle für die Meldung von vermutetem Missbrauch, Verpflichtung zur schnellen Erkennung und Beseitigung von Missbrauch (rascher Takedown) einschließlich Suspendierungen, Sicherstellung der Vollständigkeit der WHOIS-Informationen zum Zeitpunkt der Eintragung, Veröffentlichung und Unterhaltung von Verfahren für die Entfernung von Orphan Glue Records für Namen, die aus der Zone entfernt wurden, und Ergreifung von Maßnahmen zur Abschreckung von WHOIS-Missbrauch einschließlich Rate Limit, Feststellung der Syntaxgültigkeit und Umsetzung und Durchsetzung von Anforderungen aus dem Registry-Registrar Agreement.

Missbräuchliche Aktivitäten während des Betriebs eines gTLD Registry-Systems können wie folgt kategorisiert werden:

- Missbräuchliche Eintragungen von Namen unter einer gTLD
- Missbräuchliche böswillige Nutzung eines Domains unter dieser gTLD („Malicious Use“)
- Missbrauch der Eintragsprozesse, der technischen Schnittstellen, der Infrastruktur der Registry-Systeme und des DNS-Netzwerks selbst

Für die erste (und teilweise auch zweite) Kategorie hat die ICANN RAPWG (Registration Abuse Policies Working Group) eine anschauliche Kategorisierung bekannter Missbrauchsarten in ihrem „Registration

Hamburg Top-Level-Domain GmbH • Gertigstraße 28 • 22303 Hamburg

Abuse Policies Working Group Final Report“ (<http://gnso.icann.org/issues/rap/rap-wg-final-report-29may10-en.pdf>, vom 29. Mai 2010) eingeführt. Die Anti-Abuse-Maßnahmen der Registry der gTLD .HAMBURG folgen weitgehend den Empfehlungen der RAPWG für die einzelnen Missbrauchsszenarien. Weitere Einzelheiten zu den einzelnen Gegenmaßnahmen folgen unten.

Außerdem berücksichtigt die geplante Registry auch die Dokumente „SAC 048“ („SSAC Comment on Orphan Glue Records in the Draft Applicant Guidebook“) und „SAC 023“ („Is the WHOIS Service a Source for email Addresses for Spammers?“) des ICANN Security and Stability Advisory Committee.

Allgemeine Bestimmungen gegen Missbrauch unter der gTLD .HAMBURG

Rechtmäßige Sicherungsmaßnahmen

Um die Anforderungen der ICANN an eine Community-basierte Bestimmung der Anwendung zu erfüllen, muss der Registrant .HAMBURG-Domains in einer wirtschaftlichen, kulturellen, sozialen oder sonstigen sinnvollen Verbindung mit der Metropolregion Hamburg benutzen.

Diese Bestimmung der gTLD .HAMBURG für die .HAMBURG-Community wird durch eine spezielle Formulierung im Registry-Registrar-Agreement durchgesetzt, die gTLD-Registren für die Berücksichtigung der oben dargelegten Einschränkungen in den entsprechenden Verträgen mit den gTLD-Registranten verantwortlich macht.

Die Registry wird eingetragene Domains gelegentlich in eigenem Ermessen oder aufgrund von Beweisen oder Hinweisen manuell ständig oder immer wieder überprüfen, um die dauerhafte Erfüllung dieser Anforderungen sicherzustellen. Bei Nichteinhaltung erfolgt eine Mitteilung, die eine Frist von 20 Tagen für die Erfüllung setzt. Nichteinhaltung nach einer solchen Mitteilung kann dazu führen, dass die entsprechende Domain nach Ermessen der Registry aufgehoben wird.

Maßnahmen bezüglich der WHOIS-Genauigkeit

Parallel zur Überprüfung von .HAMBURG-Domains auf Einhaltung der Qualifizierungsvorgaben werden diese Domains gleichzeitig auf die Genauigkeit der WHOIS-Daten geprüft.

Bestimmungen für Kontakt und Bearbeitung bei Missbrauchsfällen

Der Registry Operator von .HAMBURG wird eine einzige Kontaktstelle für Missbrauchsmeldungen auf seiner Website einrichten und veröffentlichen.

Dieser Kontakt ist für Angelegenheiten, die beschleunigt bearbeitet werden müssen, und eine zeitnahe Antwort auf Missbrauchsbeschwerden mit Bezug zu allen unter .HAMBURG eingetragenen Namen aller eingetragenen Registraren einschließlich Wiederverkäufern zuständig.

Die Kontaktdaten für den Missbrauchskontakt bestehen aus

- einer E-Mail-Adresse
- einer Telefonnummer

Hamburg Top-Level-Domain GmbH • Gertigstraße 28 • 22303 Hamburg

Tel. +49 40 6506 2020 • Fax: +49 40 6506 20229 • support@dothamburg.de • www.nic.hamburg • Geschäftsführer: Oliver Süme
Registergericht: Handelsregister am Amtsgericht Hamburg HRB 102491; Rechnungsadresse und Sitz der Gesellschaft: Gertigstraße 28, 22303 Hamburg

Finanzamt: Hamburg-Barmbek-Uhlenhorst • Steuer-Nr: 43/763/00418 • Ust-ID/VAT: DE243908951

Bankverbindung: Hamburger SPARKASSE AG • IBAN: DE2920050550102225377 • BIC: HASPDEHXXX

Hamburg Top-Level-Domain GmbH • Gertigstraße 28 • 22303 Hamburg

- der Postanschrift des Missbrauchskontakts (Sitz der Registry)

An den Missbrauchskontakt gesendete Kommunikation wird wie folgt behandelt:

- Prüfung eingehender Kommunikation für neue Missbrauchsanfragen und/oder laufende Fälle
- Entsprechende Behandlung restlicher Kommunikation wie Spam oder sachfremde Anfragen (z. B. nach Domains in anderen TLDs) z. B. durch Löschen oder Zurückweisung
- Ermittlung des Registrar der betreffenden Domain
- Vorläufige Antwort an den Anfragenden
- Kontaktaufnahme zum Registrar des Datensatzes mit dem Missbrauchsfall
- Nachvollziehen der Maßnahmen des Registrar bei Missbrauch
- Übersendung der Ergebnisse an den Anfragenden

Die Bestätigung des Kommunikationseingangs und die Weiterleitung drittparteilicher Kommunikation gehört während der Geschäftszeiten zum Tagesgeschäft, jedoch besteht eine Bearbeitungsfrist von maximal 24 Stunden. Der ursprüngliche Zeitrahmen bis zum Abschluss der Missbrauchsbehandlungsmaßnahmen beträgt für den eingetragenen Registrar 72 Stunden. In Ausnahmefällen und nur auf Verlangen des Registrar kann die Frist um weitere 24 Stunden verlängert werden. Einzelheiten dazu werden im Registrar Accreditation Agreement festgelegt.

Mögliche Kategorien des Eintragungsmissbrauchs und Gegenmaßnahmen

Wie oben dargelegt hat die ICANN RAPWG einige mögliche Missbrauchskategorien identifiziert (siehe Kapitel 5 im entsprechenden Dokument). Sie entsprechen dem ersten Aufzählungspunkt des möglichen Missbrauchs einer Registry gemäß der Liste unter Ziffer 1 oben („Missbräuchliche Eintragungen“). Das geplante Registry-System behandelt diese einzelnen Kategorien wie folgt:

Cybersquatting

Missbräuche aus Cybersquatting-Fällen in der gTLD .HAMBURG werden gemäß dem bestehenden und bekannten Uniform Dispute Resolution Process („UDRP“) der ICANN behandelt. Registry-Mitarbeiter werden auch Entwicklungen bezüglich Rechtsschutzmechanismen innerhalb der ICANN genau verfolgen und mögliche Wege in Richtung auf die Übernahme solcher Prozesse untersuchen, wenn sie für den Registry Space .HAMBURG klar definiert sind.

Front Running

Obwohl die RAPWG keine spezielle Maßnahme bei diesem Problem empfiehlt, wird die Registry a) alle Protokolldateien und andere Informationen, die Benutzerinteressen an bestimmten Domains widerspiegeln, vertraulich behandeln. Diese Daten und Protokollinformationen werden nur Mitarbeitern zur Verfügung stehen, die tatsächlich aus betrieblichen Gründen auf diese Dateien zugreifen müssen, und b) das Registrar Accreditation Agreement der gTLD wird eine entsprechende Bestimmung enthalten.

Hamburg Top-Level-Domain GmbH • Gertigstraße 28 • 22303 Hamburg

Tel. +49 40 6506 2020 • Fax: +49 40 6506 20229 • support@dothamburg.de • www.nic.hamburg • Geschäftsführer: Oliver Sürme
Registergericht: Handelsregister am Amtsgericht Hamburg HRB 102491; Rechnungsadresse und Sitz der Gesellschaft: Gertigstraße 28, 22303 Hamburg

Finanzamt: Hamburg-Barmbek-Uhlenhorst • Steuer-Nr: 43/763/00418 • Ust-ID/VAT: DE243908951

Bankverbindung: Hamburger SPARKASSE AG • IBAN: DE29200505501022225377 • BIC: HASPDEHXXX

Hamburg Top-Level-Domain GmbH • Gertigstraße 28 • 22303 Hamburg

Gripe Sites, betrügerische und beleidigende Domains

Die gTLD-Registry wird Best Practices entwickeln, um die Eintragung beleidigender Zeichenfolgen einzuschränken. Außerdem wird angenommen, dass der bestehende UDRP zusammen mit gerichtlichen Entscheidungen (durch die die Registry offenkundig gebunden sein wird) ausreichende unabhängige Maßnahmen gegen möglicherweise missbräuchliche Namen bietet.

Gefälschte Verlängerungsmitteilungen

Die Registry wird gemäß den Empfehlungen der RAPWG keine spezielle Gegenmaßnahme in ihren Systemen und Services implementieren. Da die Registry für alle Domains genaue und vollständige WHOIS-Informationen (die als Informationsquelle für solche Mitteilungen betrachtet werden) bereitstellen muss, ist die Implementierung solcher Maßnahmen auf dieser Ebene nicht realisierbar. Selbstverständlich überwacht die ICANN fortwährend dieses Problem und wird gegen Registrare, die solche Praktiken ausüben, notwendige Maßnahmen ergreifen.

Die Registry wird aber auf der Website Warnungen wegen klar betrügerischer (und klar ungesetzlicher) Verlängerungs- und Ablaufmitteilungen veröffentlichen, die ihren Mitarbeitern zur Kenntnis gelangen, und sie wird rechtliche Schritte gegen Registrare einleiten, die solche ungesetzlichen, betrügerische Handlungen durchführen.

Name Spinning

Name Spinning wird als eine hauptsächlich von Registraren rechtmäßig angewandte Praxis betrachtet, um Nutzern eine größere Auswahl und/oder Alternativen anzubieten, wenn der gewünschte Name bereits vergeben ist. Hierbei wird davon ausgegangen, dass der überlegte Einsatz dieser Techniken in der Verantwortung des Registrars liegt. Die Registry kann nicht zwischen einer rechtmäßigen Domainanfrage, also einer, die von einem Nutzer von Hand eingegeben wurde, und einer Domainanfrage die vom Registrar geändert wurde, unterscheiden.

Wenn die Name-Spinning-Praktiken zu einem Markenverstoß bei Domains führen könnten, sieht die UDRP geeignete Maßnahmen gegen den Inhaber eines solchen Namens vor. Das entspricht der Empfehlung der RAPWG.

Pay-Per-Click

In Übereinstimmung mit der Position der RAPWG wird dieses Thema, das nicht direkt mit der Eintragung von Domains in Verbindung steht, als indirekt und rein auf das Web bezogen betrachtet. In den meisten Fällen ist Pay-Per-Click eine rechtmäßige Einkommensquelle für Eigentümer von Domains und Betreiber von Websites. Möglicher Missbrauch solcher Praktiken muss außerhalb des Bereichs für die Registry liegen, und auch hier wird erwartet, dass Markenverstöße mithilfe der UDRP geregelt werden.

Traffic-Umleitung

Hamburg Top-Level-Domain GmbH • Gertigstraße 28 • 22303 Hamburg

Tel. +49 40 6506 2020 • Fax: +49 40 6506 20229 • support@dothamburg.de • www.nic.hamburg • Geschäftsführer: Oliver Sürme
Registergericht: Handelsregister am Amtsgericht Hamburg HRB 102491; Rechnungsadresse und Sitz der Gesellschaft: Gertigstraße 28, 22303 Hamburg

Finanzamt: Hamburg-Barmbek-Uhlenhorst • Steuer-Nr: 43/763/00418 • Ust-ID/VAT: DE243908951

Bankverbindung: Hamburger SPARKASSE AG • IBAN: DE29200505501022225377 • BIC: HASPDEHHXXX

Hamburg Top-Level-Domain GmbH • Gertigstraße 28 • 22303 Hamburg

In Übereinstimmung mit der Position der RAPWG ist dies ebenfalls ein Web-Thema und es wurden keine speziellen Gegenmaßnahmen in den Betriebsablauf der Registry implementiert.

Domain Kiting / Tasting

Um massenhaftes Domain Kiting/Tasting (wie es in gTLD- und ccTLD-Registries beobachtet werden konnte) zu verhindern, wird die Registry die „Add Grace Period Limits Policy“ (<http://www.icann.org/en/tlds/agp-policy-17cec08-en.htm>) implementieren, die den finanziellen Vorteil von Domain Kiting/Tasting wirkungsvoll entfernt und somit das Volumen solcher Eintragungen wesentlich verringert. Alle Registrare werden in dieser Beziehung offensichtlich gleich behandelt, und es gibt keine Ausnahmen von der Richtlinie.

Missbräuchliche Nutzung einer Domain

Entsprechend dem zweiten Aufzählungspunkt in der Liste oben („Missbräuchliche Nutzung“) hat die RAPWG ihrem Abschlussbericht auch eine Analyse beigefügt. Die Registry wird die unten beschriebene Richtlinie anwenden:

Anti-Abuse-Richtlinie für gTLD

Die Absicht hinter der Anti-Abuse-Richtlinie von .HAMBURG ist die Ergreifung von Maßnahmen gegen die Nutzung von Domains in Verbindung mit ungesetzlichen, böswilligen, betrügerischen oder auf andere Weise schädlichen Aktivitäten im Internet. Solche Aktivitäten sind:

- Spam: Spam wird allgemein als das Senden massenhafter unaufgeforderter E-Mails definiert, kann aber auch beim Instant Messaging oder in mobilen Umgebungen auftreten. Spam kann von Domains aus verschickt werden und wird als Werbung für Websites eingesetzt.
- Phishing: Phishing liegt vor, wenn sich eine Website als vertrauenswürdige Website - oft als eine Bank-Website - darstellt, um Internet-Nutzer zu täuschen, damit sie sensible Informationen (z. B. Zugangsdaten für Online-Banking, E-Mail-Passwörter) enthüllen.
- Pharming: Pharming ist die Umleitung von Internet-Nutzern auf betrügerische Websites, die vorwiegend durch Techniken wie DNS-Hijacking oder Poisoning erreicht wird.
- Absichtliche Verteilung von Malware: Malware ist Software, die das System eines Nutzers ohne dessen Einwilligung infiltriert, um ihn zu schädigen oder z. B. für Botnet-Aktivitäten zu missbrauchen. Beispiele sind Viren, Würmer, Trojaner oder Key Logger.
- Malicious Fast-Flux-Hosting:
Malicious Fast-Flux-Hosting ist eine DNS-basierte Komponente von Botnet-Aktivitäten, insbesondere um z. B. den Standort dieser Aktivitäten im Internet zu verschleiern und gegen Entdeckung und Verteidigung zu abzuwehren.

Eingehende Kommunikation über einen möglichen Missbrauch wird gemäß Abschnitt 3 der Reaktion auf diese Richtlinie behandelt. Fachleute beim Registry Operator werden beurteilen, ob tatsächlich ein

Hamburg Top-Level-Domain GmbH • Gertigstraße 28 • 22303 Hamburg

Tel. +49 40 6506 2020 • Fax: +49 40 6506 20229 • support@dothamburg.de • www.nic.hamburg • Geschäftsführer: Oliver Süme
Registergericht: Handelsregister am Amtsgericht Hamburg HRB 102491; Rechnungsadresse und Sitz der Gesellschaft: Gertigstraße 28, 22303 Hamburg

Finanzamt: Hamburg-Barmbek-Uhlenhorst • Steuer-Nr: 43/763/00418 • Ust-ID/VAT: DE243908951

Bankverbindung: Hamburger SPARKASSE AG • IBAN: DE2920050550102225377 • BIC: HASPDEHXXX

Hamburg Top-Level-Domain GmbH • Gertigstraße 28 • 22303 Hamburg

Missbrauch in Zusammenhang mit einem gTLD-Domains vorliegt und welcher Art er ist. Danach wird die beste Methode zur Beseitigung des Problems von der Erstbeurteilung abgeleitet.

Die Hauptunterschiede sind a) ob die Domains eigens zur Durchführung der böswilligen Aktivität eingetragen wurde oder die Aktivität eine rechtmäßige Nutzung der Domains ausbeutet und der Registrant absolut keine Kenntnis davon hat, d. h. die Website gehackt wurde, und b) ob eine sofortige Maßnahme notwendig ist (Domain wird gesperrt und aus der Zone entfernt) oder nicht (Domain wird nur gesperrt).

Die Registry wird über Missbrauch und Missbrauchsmeldungen Aufzeichnungen aufbewahren und Metriken nachverfolgen. Dazu gehört

- die Anzahl der beim oben beschriebenen Missbrauchskontakt der Registry eingegangenen Missbrauchsmeldungen;
- die Anzahl der Fälle und Domains, die Registraren zur Lösung überstellt wurden;
- die Anzahl der Fälle und Domains, in denen die Registry Sofortmaßnahmen ergriffen hat;
- die Zeit für die Lösung;
- die Anzahl der Domains in der gTLD, die von den größeren Anti-Spam Blocklist Providern auf eine schwarze Liste gesetzt wurden, und
- die Zeiten, in denen Phishing-Sites in der gTLD aktiv und offen waren.

Behandlung von URS-Anfragen

Die Behandlung von Uniform Rapid Suspension-Anfragen (URS-Anfragen) durch den Registry Operator ist oben ausführlich dargestellt.

Missbrauch von Registry-Schnittstellen

Die Registry wird die folgenden Gegenmaßnahmen zum Schutz gegen Missbrauch der Registry-Systeme und des DNS-Netzwerks selbst ergreifen:

Abgreifen von WHOIS-Daten

WHOIS-Zugriff ist ein entscheidender und unverzichtbarer Service, den jede gTLD-Registry erbringt, und die Registry wird die ICANN-Anforderungen für den WHOIS-Zugriff erfüllen.

Wie im Dokument „Is the WHOIS Service a Source for email Addresses for Spammers?“ der SSAC dargelegt, kann der Missbrauch von WHOIS als das Hauptmittel für die Generierung von E-Mail-Adresslisten zum Versenden unaufgeforderter E-Mails betrachtet werden, insbesondere für die Praxis, massenhaft Informationen bei WHOIS abzugreifen. Auch wird angenommen, dass WHOIS die Hauptquelle für Daten zur Generierung falscher Verlängerungsmittelungen ist. Zum Schutz gegen das Abgreifen von Eintragsdaten (und insbesondere E-Mail-Adressen) wird die Registry die folgenden Gegenmaßnahmen ergreifen:

Hamburg Top-Level-Domain GmbH • Gertigstraße 28 • 22303 Hamburg

Tel. +49 40 6506 2020 • Fax: +49 40 6506 20229 • support@dothamburg.de • www.nic.hamburg • Geschäftsführer: Oliver Süme
Registergericht: Handelsregister am Amtsgericht Hamburg HRB 102491; Rechnungsadresse und Sitz der Gesellschaft: Gertigstraße 28, 22303 Hamburg

Finanzamt: Hamburg-Barmbek-Uhlenhorst • Steuer-Nr: 43/763/00418 • Ust-ID/VAT: DE243908951

Bankverbindung: Hamburger SPARKASSE AG • IBAN: DE29200505501022225377 • BIC: HASPDEHXXX

Hamburg Top-Level-Domain GmbH • Gertigstraße 28 • 22303 Hamburg

- Rate Limits für die WHOIS-Abfrage: Der Zugriff auf WHOIS-Daten für Abfragen wird pro IP-Adresse (für IPv4) und pro Präfix (für IPv6) auf eine tägliche Obergrenze von 25 WHOIS-Abfragen pro IP-Adresse/Präfix eingeschränkt. Nach Erreichen der Obergrenze antwortet der WHOIS-Server mit einer entsprechenden Mitteilung anstelle der standardmäßigen WHOIS-Antwort. (Die Abfrageobergrenzen können vom Registry Operator gelegentlich geprüft und angepasst werden). IP-Bereiche akkreditierter Registraren (und andere IP-Bereiche wie z. B. ICANN selbst, UDRP- und URS-Service Provider usw.) werden von diesen Einschränkungsmaßnahmen ausgenommen. Dadurch wird die rechtmäßige Nutzung des Service ermöglicht, während das Abgreifen von Daten in großem Maßstab gleichzeitig sehr erschwert wird.
- Datenschutz bei E-Mail/Telefon/Fax: Die EPP-Implementierung des „Kontaktobjekts“ bietet einen Mechanismus, über den ein Registrar definieren kann, ob die Felder „email“, „phone“ und „fax“ des Kontaktobjekts (d. h. das Element „contact:disclose“) öffentlich angezeigt werden. Die Registry setzt diese Felder standardmäßig auf „do not disclose“, aber Registrare können diese Einstellung über den normalen EPP Command Stream ändern. Ist ein Flag für ein bestimmtes Feld auf „do not disclose“ gesetzt, wird das Feld bei anonymen WHOIS-Ausgaben weggelassen und so ein Mindestmaß an Datenschutz für Registranten erreicht. Um verschiedene Geschäftsprozesse zuzulassen, werden IP-Bereiche akkreditierter Registrare (und gegebenenfalls andere IP-Bereiche wie z. B. ICANN selbst, UDRP- und URS-Service Provider) den vollständigen Datensatz einschließlich der mit „do not disclose“ markierten Felder immer noch sehen müssen.
- Überwachung von WHOIS: Der WHOIS-Service wird überwacht, um ungewöhnliche Aktivitäten an der Schnittstelle zu erkennen.

Die oben beschriebenen Gegenmaßnahmen sind ein ausgewogener Kompromiss zwischen den Anforderungen, Zugriff auf WHOIS-Daten zu bieten, und den grundlegenden Datenschutzrechten von Registranten. Weitere Informationen über den von der Registry erbrachten WHOIS-Service sind im Vertrag der Registry mit ICANN enthalten.

Missbrauch der EPP-Schnittstelle

Die EPP-Schnittstellen der Registry werden sehr stark durch Firewalls geschützt, und Zugriff besteht nur aus IP-Bereichen akkreditierter Registraren; außerdem werden sie noch durch einen EPP-Authentifizierungsmechanismus geschützt. Als solcher kann ein Missbrauch dieser Schnittstellen (wie DDoS, Brute-Force-Angriffe gegen Benutzernamen/Passwort-Kombinationen usw.) nur von Netzwerken von Parteien aus durchgeführt werden, mit denen der Registry Operator einen rechtsgültigen Vertrag geschlossen hat. Außerdem gilt für EPP-Schnittstellen auf Netzwerkebene ein Rate Limit.

Zusätzlich zu den dargelegten technischen Mitteln werden Nutzungszahlen jenseits aller regelmäßigen und sinnvollen Abrufmuster, die gerade anfallen oder regelmäßig auftreten, vom Registry Operator untersucht. Das Fehlen einer vernünftigen Erklärung für ein solches unregelmäßiges Verhalten eines Registrars an der EPP-Schnittstelle könnte zu Strafen wie Herabstufung des Service, Unterbrechung oder sogar Kündigung im gemäß dem Registrar Accreditation Agreement vorgesehenen maximalen Umfang führen.

Hamburg Top-Level-Domain GmbH • Gertigstraße 28 • 22303 Hamburg

Tel. +49 40 6506 2020 • Fax: +49 40 6506 20229 • support@dothamburg.de • www.nic.hamburg • Geschäftsführer: Oliver Süme
Registergericht: Handelsregister am Amtsgericht Hamburg HRB 102491; Rechnungsadresse und Sitz der Gesellschaft: Gertigstraße 28, 22303 Hamburg

Finanzamt: Hamburg-Barmbek-Uhlenhorst • Steuer-Nr: 43/763/00418 • Ust-ID/VAT: DE243908951

Bankverbindung: Hamburger SPARKASSE AG • IBAN: DE2920050550102225377 • BIC: HASPDEHXXX

Missbrauch der DNS-Schnittstelle

Öffentliche Namensserver, Hidden Masters und die Signing-Infrastruktur werden so konfiguriert und durch Firewalls geschützt, dass sie NOTIFYs und UPDATEs nur von den erforderlichen Adressen zulassen. Um das Überschreiten von Zonen und Ladespitzen zu verhindern, sind Zonenübertragungen aus der DNS-Infrastruktur deaktiviert.

Verwaltung und Entfernung von Orphan Glue Records

Selbstverständlich haben Glue Records gemäß den Kommentaren der SSAC unter <http://www.icann.org/en/committees/security/sac048.pdf> eine wichtige Funktion beim korrekten und normalen Betrieb des DNS, können aber für böswillige Zwecke eingesetzt werden.

Um eine solche böswillige Nutzung zu verhindern, verwaltet die Registry Glue Records gemäß der folgenden Richtlinie:

- Bereitstellung von Host-Objekten mit Glue: Gemäß den EPP RFCs können Glue-Record-Hostobjekte („intern“) nur bereitgestellt werden, wenn die übergeordnete Domain (Parentname) in der Registry eingetragen ist. Für Hostobjekte, die von der Registry nicht unter der TLD verwaltet werden („externe Hosts“) können niemals A- oder AAAA-Datensätze existieren.
- Löschung der Domäne bei untergeordneten Glue-Record-Hosts: Wenn sich der Status einer Domain (zum Beispiel über den EPP-Befehl „delete domain“ oder durch Ablauf) von „REGISTERED“ in „REDEMPTION“ ändert, wird zwar die Domain selbst aus dem DNS entfernt, aber Glue Records in der gelöschten Domain werden vorübergehend in der Zone gehalten. Andere Registrare, die aufgrund der anstehenden Entfernung des Hosts aus ihren Domains von einer möglichen Auswirkung auf den DNS-Service betroffen sind, werden über die EPP-Nachrichtenschlange informiert.
- Wenn sich der Status der Domain danach von „REDEMPTION“ in „PENDING DELETE“ ändert, werden die Glue Records unter den betroffenen Domains dann im DNS widerrufen, sind aber in der SRS-Datenbank immer noch vorhanden.
- Im letzten Schritt des Löschvorgangs (Übergang von „PENDING DELETE“ zu „AVAILABLE“) werden die Glue-Record-Hostobjekte zusammen mit der Domain gelöscht und auch aus jeder anderen Domain in der Registry entfernt, der diese Hosts noch nutzt.
- Diese Richtlinie verhindert wirkungsvoll den Missbrauch von Orphan Glue Records in der Registry, da der Status eines Hostobjekts immer dem Status der übergeordneten Domain folgt. Daher können Glue Records niemals für Domains existieren, die nicht in der Registry-Datenbank vorhanden sind. Außerdem verringert die Beibehaltung der Glue Records in der Zone während der Rücknahmepériode zusammen mit der Benachrichtigung von Registraren wesentlich das Risiko anderer Domains beeinträchtigt zu werden sowie den Aufwand eines Registrars für den Fall, dass die Domain nachträglich wiederhergestellt wird.

Hamburg Top-Level-Domain GmbH • Gertigstraße 28 • 22303 Hamburg

Zusätzlich zu der oben dargelegten Verfahrensweise wird der Registry Operator auch auf dokumentierte Beweise für das Vorhandensein von Glue Records und deren Verwendung in Verbindung mit böswilligen Aktivitäten hin handeln und die Glue Records manuell entfernen.

Kontakte

Alle Missbrauchsmeldungen sind an abuse@nic.HAMBURG zu senden.

Beschwerden wegen ungenauer WHOIS-Informationen sind an den Registrar dieser Domain zu richten. Beschwerden können auch an whois@nic.HAMBURG gesendet werden.

Hamburg Top-Level-Domain GmbH • Gertigstraße 28 • 22303 Hamburg

Tel. +49 40 6506 2020 • Fax: +49 40 6506 20229 • support@dothamburg.de • www.nic.hamburg • Geschäftsführer: Oliver Sürme
Registergericht: Handelsregister am Amtsgericht Hamburg HRB 102491; Rechnungsadresse und Sitz der Gesellschaft: Gertigstraße 28, 22303 Hamburg

Finanzamt: Hamburg-Barmbek-Uhlenhorst • Steuer-Nr: 43/763/00418 • Ust-ID/VAT: DE243908951

Bankverbindung: Hamburger SPARKASSE AG • IBAN: DE29200505501022225377 • BIC: HASPDEHXXX