tldbox GmbH
Jakob-Haringer-Str. 8/V · 5020 Salzburg · Austria
T +43 662 46 69 -731 · F -29
service@nic.versicherung · **www.nic.versicherung**

Anti-Abuse-Richtlinie für .versicherung Domains

Übersicht

1 Vorwort

Die folgende Richtlinie („.versicherung Anti-Abuse-Richtlinie“) wird gemäß dem Vertrag zwischen Registry und Registrar (Registry-Registrar-Agreement, „RRA“) eingeführt. Die missbräuchliche Verwendung von .versicherung-Domains wird nicht toleriert.
Die Richtlinie behandelt die allgemeinen Aspekte der Verhinderung missbräuchlicher Verwendung, akzeptabler Nutzung und rascher Erkennung und Verfolgung (rasche Entfernung); sie gilt für Registrare und Registranten von .versicherung-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 unter der gTLD .versicherung auf eine Weise genutzt wird, 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. Die Nichteinhaltung der obigen Bestimmungen kann zur Aussetzung oder Aufhebung der Domainregistrierung durch die Registry führen.

Die Registry wird zusammen mit dem Registrar die erforderlichen betrieblichen und technischen Schritte zur Förderung der Richtigkeit der Registrant-Daten unternehmen, Domainmissbrauch einschränken, veraltete und ungenaue Daten entfernen und andere Sicherheitsmaßnahmen zur Sicherstellung der Integrität des Namensraums .versicherung ergreifen. Zu den speziellen Maßnahmen gehören neben der Anti-Abuse-Richtlinie, die Missbrauch deutlich definiert, Informationen über eine Kontaktstelle für die Meldung von vermutetem Missbrauch, die Verpflichtung zur schnellen Erkennung und Beseitigung von Missbrauch (rasche Entfernung) einschließlich Suspendierungen, Sicherstellung der Vollständigkeit der Domain-Inhaber-Informationen zum Zeitpunkt der Registrierung, Ver-

öffentlichung und Unterhaltung von Verfahren für die Entfernung von „Orphan Glue Records“ für Namen, die aus der Zone entfernt wurden, und die 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 einer Domain unter dieser gTLD („Malicious Use“)
- Missbrauch der Eintragungsprozesse, 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 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 .versicherung folgen weitgehend den Empfehlungen der RAPWG für die einzelnen Missbrauchsszenarien. Weitere Einzelheiten zu den einzelnen Gegenmaßnahmen siehe unten.

2 Allgemeine Bestimmungen gegen Missbrauch unter der gTLD .versicherung

2.1 Rechtmäßige Sicherungsmaßnahmen

Um die Anforderungen der ICANN an eine Community-basierte Bestimmung der Anwendung zu erfüllen, muss der Registrant die .versicherung-Domain in einer sinnvollen Verbindung mit der deutschsprachigen Versicherungsindustrie nutzen.
Diese Bestimmung der .versicherung-Domains für die deutschsprachige Versicherungs-Community wird durch eine spezielle Formulierung im Registry-Registrar-Agreement durchgesetzt, die gTLD-Registrare für die Berücksichtigung der oben dargelegten Einschränkungen in den entsprechenden Verträgen mit den gTLD-Registranten verantwortlich macht.
Die Registry validiert jeden Registranten, um sicherzustellen, dass die Registrierungsvoraussetzungen dieser Richtlinie für .versicherung-Domains erfüllt werden. Die Überprüfung erfolgt erstmals nach technisch erfolgreicher Registrierung und wird jährlich wiederholt.

Ist die Einhaltung der Registrierungs-Policy fraglich erfolgt eine Mitteilung, die eine Frist von 30 Tagen für den entsprechenden Nachweis setzt. Nichteinhaltung nach einer solchen Frist kann dazu führen, dass die entsprechende Domain nach Ermessen der Registry technisch funktionsunfähig gesetzt wird (Server Hold).

2.2 Maßnahmen bezüglich der Richtigkeit der Registrant-Daten

Domains können jederzeit auf die Richtigkeit ihrer Registrant-Daten geprüft werden.

2.3 Bestimmungen für Kontakt und Bearbeitung bei Missbrauchsfällen

Der Registry-Operator von .versicherung veröffentlicht eine Kontaktstelle für Missbrauchsmeldungen auf seiner Website. Diese Kontaktstelle ist für Angelegenheiten, die beschleunigt bearbeitet werden müssen, und eine zeitnahe Antwort auf Missbrauchsbeschwerden mit Bezug zu allen unter .versicherung eingetragenen Namen aller eingetragenen Registrare einschließlich Wiederverkäufern zuständig.

Die Kontaktdaten für den Missbrauchskontakt bestehen aus:

- einer E-Mail-Adresse
- einer Telefonnummer
- der Postanschrift des Missbrauchskontakts (Sitz der Registry)

Die an den Missbrauchskontakt gesendete Kommunikation wird folgendermaßen behandelt:

- Prüfung eingehender Kommunikation für neue Missbrauchsfragen 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 Registrars der betreffenden Domain
- Vorläufige Antwort an den Anfragenden
- Kontaktaufnahme zum Registrar des Datensatzes mit dem Missbrauchsfall
- Dokumentation der Maßnahmen der Registry und des Registrars bei Missbrauch
- Erforderlichenfalls Information der zuständigen Behörden, z. B. Polizei und/oder Staatsanwaltschaft
- 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 Registrars kann diese Frist um weitere 24 Stunden verlängert werden. Einzelheiten dazu werden im Registrar Accreditation Agreement festgelegt.

3 Mögliche Kategorien des Registrierungsmissbrauchs 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 Registry-System behandelt diese einzelnen Kategorien wie folgt:

a. Cybersquatting

Missbräuche aus Cybersquatting-Fällen in der gTLD .versicherung werden gemäß dem Uniform Dispute Resolution Process („UDRP“) der ICANN behandelt. Jedoch werden Registry-Mitarbeiter auch Entwicklungen bezüglich Rechtsschutzmechanismen innerhalb der ICANN genau folgen und mögliche Wege in Richtung Übernahme solcher Prozesse untersuchen, wenn sie klar definiert sind.

b. Front Running

Obwohl die RAPWG keine spezielle Maßnahme bei diesem Problem empfiehlt, wird die Registry

- alle Protokolldateien und andere Informationen, die Benutzerinteressen an einer bestimmten Domain widerspiegeln, vertraulich behandeln. Diese Daten und Protokollinformationen werden nur Mitarbeitern zur Verfügung stehen, die tatsächlich aus betrieblichen Gründen auf diese Dateien zugreifen müssen und
- das Registrar Accreditation Agreement der gTLD wird eine entsprechende Bestimmung enthalten.

c. Gripe Sites; betrügerische und beleidigende Domains

Die .versicherung-Registrierungs-Policy sieht vor, dass Domains nicht beleidigend oder betrügerisch sein dürfen. Außerdem wird festgehalten, dass der bestehende UDRP zusammen mit gerichtlichen Entscheidungen (an die die Registry gebunden ist) ausreichende unabhängige Maßnahmen gegen möglicherweise missbräuchliche Namen bietet.

d. Gefälschte Verlängerungsmitteilungen

Die .versicherung-Registry wird gemäß den Empfehlungen der RAPWG keine spezielle Gegenmaßnahme in ihren Systemen und Services implementieren. Selbstverständlich überwacht aber ICANN dieses Problem laufend und wird gegen Registrare, die solche Praktiken ausüben, notwendige Gegenmaßnahmen ergreifen. Die .versicherung-Registry behält sich vor, rechtliche Schritte gegen Registrare einzuleiten, die solche illegalen, betrügerischen Handlungen setzen.

e. 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. Der überlegte Einsatz dieser Techniken liegt in der Verantwortung des Registrars. In der Praxis ist es der Registry nicht möglich, zwischen einer rechtmäßigen Domainanfrage, also einer, die von einem Nutzer von Hand eingegeben wurde, und einer Domainanfrage, die vom Registrar geändert wurde, zu unterscheiden.

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

f. 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 liegt außerhalb des Bereichs für die Registry. Auch hier können Markenverstöße mithilfe der UDRP geregelt werden.

g. Traffic-Umleitung

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.

h. Domain Kiting / Tasting

Die .versicherung-Registry wird die .versicherung-Community und Registrare über die Registrierungs-Policy informieren, um die mögliche Verwirrung der Nutzer und Fehlregistrierungen möglichst gering zu halten.

i. Missbräuchliche Nutzung einer Domain

Entsprechend Punkt 2 der obigen Liste („Missbräuchliche Nutzung“) hat die RAPWG ihrem Abschlussbericht auch eine Analyse beigefügt. Die Registry wird die unten beschriebene Richtlinie anwenden:

Die Absicht hinter der Anti-Abuse-Richtlinie von .versicherung ist die Ergreifung von Maßnahmen gegen die Nutzung von Domains in Verbindung mit illegalen, böswilligen, betrügerischen oder auf andere Weise schädliche 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.
- 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 es 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 abzuhärten.

Eingehende Kommunikation über einen möglichen Missbrauch wird gemäß Abschnitt 2.3 dieser Richtlinie behandelt. Fachleute der Registry werden in weiterer Folge beurteilen, ob tatsächlich ein Missbrauch in Zusammenhang mit einer gTLD-Domain vorliegt und welcher Art er ist. Danach wird die beste Methode zur Beseitigung des Problems von der Erstbeurteilung abgeleitet.

Die Hauptunterschiede sind

- ob die Domains eigens zur Durchführung der böswilligen Aktivität eingetragen wurden oder
- die Aktivität eine rechtmäßige Nutzung der Domain ausbeutet und der Registrant keine Kenntnis davon hat, d. h. die Website gehackt wurde, und
- 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 dem zuständigen Registrar zur Lösung weitergeleitet wurden;
- Die Anzahl der Domains, die auf Server-Hold gesetzt wurden;
- die Anzahl der Fälle und Domains, in denen die Registry Sofortmaßnahmen ergriffen hat;
- Domains mit neuen Security-Incidents.

j. Behandlung von URS-Anfragen

Die Behandlung von Uniform Rapid Suspension-Anfragen (URS-Anfragen) durch den Registry-Operator erfolgt gemäß den Vorgaben von ICANN.

k. Missbrauch von Registry-Schnittstellen

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

i. Abgreifen von WHOIS-Daten

Der WHOIS-Zugriff ist ein Service, den die gTLD-Registry erbringt, wobei die ICANN-Anforderungen für den WHOIS-Zugriff entsprechend erfüllen werden. Diesbezüglich wird auf die Whois Richtlinie für .versicherung-Domains verwiesen.

Zum Schutz gegen Missbrauch veröffentlichter Daten wird die Registry die folgenden Gegenmaßnahmen ergreifen:

- 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 Registrare (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 erschwert wird.
- Datenschutz: Grundsätzlich werden seit dem Inkrafttreten der DSGVO (https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32016R0679) in der Whois die Daten des Registranten sowie der Domain Contacts nur mehr auf explizite Beauftragung des Registrars durch den Registranten angezeigt. Die Verantwortung dafür liegt beim Registrar. Die EPP-Implementierung des „Kontaktobjekts" bietet einen Mechanismus, über den ein Registrar definieren kann, ob einzelne Felder des Kontaktobjekts (d. h. das Element „contact:disclose") öffentlich angezeigt werden. Ist ein Flag für ein bestimmtes Feld auf „do not disclose" gesetzt, wird der Feld-Inhalt bei der WHOIS-Anzeige weggelassen. Um verschiedene Geschäftsprozesse zuzulassen, können (auf Basis spezieller IP-Bereiche) akkreditierte Registrare (und gegebenenfalls andere wie z. B. ICANN selbst, UDRP- und URS-Service-Provider) den vollständigen Datensatz, einschließlich der mit „do not disclose" markierten Felder weiterhin einsehen.
- 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.

ii. Missbrauch der EPP-Schnittstelle

Die EPP-Schnittstellen der Registry sind durch Firewalls geschützt und der Zugriff besteht nur aus IP-Bereichen akkreditierter Registrare; zudem werden die Schnittstellen noch durch einen EPP-Authentifizierungsmechanismus geschützt. Als solcher kann ein Missbrauch dieser Schnittstellen (wie DDoS, Brute-Force-Angriffe gegen Benutzername/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.

iii. Missbrauch der DNS-Schnittstelle

Öffentliche Nameserver, 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.

l. Verwaltung und Entfernung von Orphan Glue Records

Selbstverständlich haben Glue Records gemäß den Kommentaren der SSAC unter https://www.icann.org/en/committees/security/sac048.pdf, eine wichtige Funktion beim korrekten und normalen Betrieb des DNS, können aber auch 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 AAA-Datensätze existieren.
- Löschung der Domain bei untergeordneten Glue-Record-Hosts: Wenn sich der Status einer Domain (zum Beispiel über den EPP-Befehl „delete domain“) von „REGISTERED“ auf „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 mittels EPP Message Queue 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 Rücknahmeperiode zusammen mit der Benachrichtigung von Registraren wesentlich das Risiko anderer Domains, beeinträchtigt zu werden sowie den Aufwand eines Registrars im Fall, dass die Domain nachträglich wiederhergestellt wird.

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.

m. Kontakte

Alle Missbrauchsmeldungen sind an abuse@nic.versicherung zu senden, alternativ kann die Registry telefonisch unter +43 662 46 69 -731 oder postalisch unter tldbox GmbH, Jakob-Haringer-Strasse 8, 5020 Salzburg, Austria erreicht werden.