VERBAND DER INTERNETWIRTSCHAFT E.V.

Hintergrundpapier zum Thema Fake-Shops

Berlin, 10. Februar 2020

Der Marktwächter „Digitale Welt“ hat das Thema „Fake-Shops“ zur Diskussion gestellt. Die Verbraucherschutzministerkonferenz (VSMK) hat im Mai 2019 das Thema ebenfalls adressiert und eine Beschlusslage zum Umgang mit Fake Shops hergestellt. Zuletzt hatte der Bundesrat im Dezember 2019 einen Entschließungsantrag verabschiedet.

I. Versuch einer Problembeschreibung

Der Begriff „Fake-Shop“ ist nicht eindeutig definiert. Eine gesetzliche Beschreibung von „Fake-Shops“ existiert nicht. Das Verständnis von „Fake-Shops“ divergiert je nachdem welcher Personenkreis danach befragt wird.

Als Arbeitsdefinition dürften insbesondere Angebote und Internetauftritte gemeint sein, über die Straftaten zum Nachteil des Kunden begangen werden.

In Betracht kommen folgende Szenarien:

- Angebote / Internetauftritte, die mit Namen und / oder Corporate Design bekannter Marken, Shops bzw. Marktplätze auftreten und nach Abschluss des Bestellvorgangs und Zahlung durch den Kunden keine oder gefälschte Waren versenden.
- Angebote / Internetauftritte, die trotz erfolgreichem Bestell und Zahlungsvorgang in betrügerischer Absicht keine Ware liefern.
- Angebote / Internetauftritte, die in betrügerischer Absicht vorgeben, als Shop zu fungieren, aber lediglich die Daten der Nutzerinnen und Nutzer sammeln, aber letztendlich keine Transaktionen ermöglichen.

II. Forderungen der Verbraucherschutzministerkonferenz (VSMK)

Die Verbraucherschutzministerkonferenz hat einen Beschluss mit Empfehlungen an die bundespolitische Ebene getroffen.

Der Beschluss wird durch zwei Punkte geprägt:

- Zum einen soll künftig eine Identitätsprüfung in das Verfahren der Domainregistrierung einer.de Domain integriert werden.
- Zum anderen soll auf selbstverpflichtender Basis ein „notice and action“ Verfahren durch die Registries sichergestellt werden.

Im Zuge der weiteren Diskussionen und Beratungen sollte die Erfahrung der Internetwirtschaft zur Berücksichtigung kommen. Hierbei möchte eco auf die nachfolgenden Aspekte hinweisen.

III. Vorgaben für generische Top Level Domains

Die Forderung nach einer Änderung und Erschwerung oder die Einführung einer Identitätsprüfung im Vorfeld der Registrierungsmöglichkeit einer Domain stellt eine tiefgreifende Veränderung der etablierten und bewährten Prozesse bei der Bereitstellung von Domains durch die Registries dar.

Bei der von der DENIC betriebenen Top Level Domain „.de“ handelt es sich um eine so genannte „country code Top Level Domain“ (ccTLD), für die der jeweilige Betreiber bestimmt, welchen Auflagen Registrare und Nutzer unterworfen sind.

Im Gegensatz dazu sind für so genannte „generic Top Level Domains“ (gTLD) wie „.com“, „.net“ oder „.berlin“ die bei der Internet Corporation for Assigned Names & Numbers entwickelten Vorgaben verbindlich. Die Entwicklung dieser Vorgaben bei ICANN folgt dem Multistakeholder-Ansatz, bei dem basisdemokratisch neben den Registries, die zentral eine Top Level Domain verwalten, den Registraren, die Kunden Domainregistrierungen ermöglichen, auch Nutzervertreter und ein Regierungsbeirat mitwirken.

Während der Verhandlungen über eine Neufassung des Akkreditierungsvertrages für Registrare im Jahr 2012 wurden insbesondere durch den Regierungsbeirat und Vertreter der Strafverfolgungsbehörden Rufe danach laut, Domainregistrierungen lediglich nach vorher erfolgter Validierung der Domainregistrierungsdaten zu ermöglichen. Zur Begründung wurde die Verhinderung strafbarer Handlungen, die einfachere Verfolgbarkeit von Tätern und der Verbraucherschutz angeführt. Letztlich wurde dies verworfen und stattdessen eine Validierung eines Datums für den Domaininhaber innerhalb einer bestimmten Frist nach erfolgter Domainregistrierung in das Vertragswerk zwischen ICANN und den Registraren aufgenommen[1]. Die Vorgaben enthalten auch eine Eskalationsprozedur für den Fall, dass eine Validierung binnen der vorgegebenen Fristen scheitert. Beachtenswert ist daran, dass eine Abwägung der verschiedenen Optionen dazu führte, einen Ansatz zur Erhöhung des Schutzniveaus zu wählen, der nicht die schnelle Verfügbarkeit von Domains einschränkt.

Die schnelle Verfügbarkeit von Domains ermöglicht nicht nur geschäftliche Aktivitäten, sondern auch die Veröffentlichung von Informationen oder Diensten. Eine Validierung von Registrantendaten ist zwangsläufig mit Verzögerungen verbunden.

IV. Erkennung/Identifizierung eines Fake-Shops

Grundsätzlich ist ein schnelles und effektives Vorgehen als Reaktion auf bekannt gewordene betrügerische Angebote auch im Interesse von Registries und der weiteren Internetwirtschaft. Fake-Shops und betrügerische Websites verursachen finanziellen Schaden und untergraben das Vertrauen in den digitalen Handel über das Internet.

[1] vgl. https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en und dort Punkt 2, die „Whois Accuracy Program Specification“

Voraussetzung für ein erfolgreiches Vorgehen gegen Fake-Shops und betrügerische Websites ist es, diese sicher zu identifizieren.

Dies kann nur anhand verschiedener Kriterien erfolgen und hängt auch stark davon ab, welche rechtswidrigen Handlungen tatsächlich begangen werden. Nicht jede verspätete oder ausbleibende Lieferung weist nach, dass es sich um ein betrügerisches Angebot handelt. Es kann sich gleichermaßen um ein technisches oder organisatorisches Problem des Anbieters handeln. Dies gilt ebenso für ausbleibende oder verzögerte Kommunikation seitens des Anbieters.

Plagiierte Produkte können ein Hinweis auf ein rechtswidriges Angebot darstellen. Allerdings lassen sich Plagiate nur schwer identifizieren. Unklar ist zudem, ob der Verkäufer ein Plagiat in betrügerischer Absicht verkauft hat, oder selbst geschädigt worden ist.

Ein fehlendes Impressum oder die Nichteinhaltung der fernabsatzrechtlichen Informationspflichten kann bestenfalls ein Indiz für ein rechtswidriges Angebot sein. Die Verwendung von Gütesiegeln wie „Trusted Shops“, Markenzeichen oder sonstigen Logos umgekehrt kann, muss aber nicht zwingend auf seriöse Angebote hinweisen. Es bleibt das Risiko, dass das Gütesiegel rechtswidrig verwendet wird.

Insgesamt kann daher festgehalten werden, dass eine eindeutige Entscheidung darüber, ob ein Angebot rechtswidrig und ein Fake-Shop ist, nicht ohne weitere Recherchen und Maßnahmen, wie etwa einen Testkauf, möglich und im Voraus feststellbar ist.

Registries, Registare oder auch Hosting Provider sind kaum imstande, eine solche Feststellung zu treffen.

V. Handlungsmöglichkeiten von Registries und Registraren

Eine Registry wie die DENIC hat keine Möglichkeit der Einflussnahme auf Inhalte von Angeboten. Beim Abruf einer Website geschehen vom Nutzer unbemerkt zwei verschiedene Vorgänge, die durch die Browsersoftware durchgeführt werden. Im ersten Schritt wird über das Domain Namen System „nachgefragt“, welche IP-Adresse zur angefragten Domain gehört. Im zweiten Schritt wird dann mit der IP-Adresse die Website aufgerufen.

Technisch sind das zwei getrennte Vorgänge und das Hosting des eigentlichen Angebots kann, muss aber keinesfalls beim selben Anbieter erfolgen. Registries und Registrare können lediglich binär entweder eine Domain zu einer IP-Adresse auflösen lassen oder dies unterbinden. Wenn die Auflösung einer Domain unterbunden wird, dann ist über die betreffende Domain ein Angebot nicht mehr erreichbar. Über andere Domains, die etwaig auf ein Angebot verweisen oder mittels der IP-Adresse ist das Angebot weiterhin verfügbar.

Wenn Domains etwa für verschiedene Angebote verwendet werden, von denen lediglich eines zu beanstanden ist, dann sind Registries und Registrare technisch nicht in der Lage, lediglich bestimmte Inhalte oder Angebote „abzuschalten“ und andere aufrechtzuerhalten. Auch bei Transaktionen über bekannte Plattformen kommt es immer wieder zu Nutzerbeschwerden und auch zum Vorwurf von

betrügerischen Angeboten. Die Domains solcher Anbieter insgesamt aus dem Domain Namen System zu tilgen wäre jedoch unverhältnismäßig. Sicherlich ist in bestimmten Fällen angezeigt, Domains „aus dem DNS“ zu nehmen. Dies sollte allerdings an besondere Voraussetzungen geknüpft werden.

Einige Registries haben statistische Verfahren entwickelt, um bei gelöschten und sodann wieder registrierten Domains zu prüfen, ob diese mit einer großen Wahrscheinlichkeit für rechtswidrige Zwecke genutzt werden könnten. Unter bestimmten Voraussetzungen werden Domains erst gar nicht technisch verfügbar gemacht. Die Effektivität dieser Maßnahmen ist derzeit nicht abschließend geklärt.

VI. eco Position

Wie einleitend bereits skizziert wurde, wird mit dem Beschluss der VSMK und des Bundesrats in erster Linie eine Änderung und Erschwerung des Registrierungsprozesses beispielsweise durch die Integration eines Identitätsprüfverfahrens sowie die Verpflichtung der Registries für die Einführung eines „notice and action“ Verfahren angeregt. Von dem Beschluss der VSMK und dem Bundesrat sind vor allem die Registries wie z. B. die DENIC betroffen.

- Integration einer Identitätsprüfung zur Domainregistrierung

Die Forderung nach einer Änderung und Erschwerung oder die Einführung einer Identitätsprüfung im Vorfeld der Registrierungsmöglichkeit einer Domain stellt eine tiefgreifende Veränderung der etablierten und bewährten Prozesse bei der Bereitstellung von Domains durch die Registries dar.

Aus diesem Grunde muss gefragt werden, ob die Änderung und Erschwerung des Registrierungsprozesses überhaupt ein geeignetes Mittel ist, um effektiv gegen betrügerische Webseiten vorzugehen.

Nach unserer Auffassung kann durch eine Erschwerung des Registrierungsprozesses nicht effektiv gegen Fake-Shops vorgegangen werden. Rechtsverletzende Angebote können leicht über alternative Endungen von Registries verfügbar gemacht werden, die weniger aufwändigen Registrierungsprozessen unterliegen, wie etwa „.com“, einer Endung, die weltweit am häufigsten registriert wird und ebenfalls ein erhebliches Nutzervertrauen genießt.

Die von der VSMK und dem Bundesrat angeregte Einführung einer Identitätsprüfung im Zuge der.de Domainregistrierung muss kritisch hinterfragt werden. Eine Identitätsprüfung im Vorfeld der Registrierungsmöglichkeit einer Domain stellt eine tiefgreifende Veränderung der etablierten und bewährten Prozesse dar.

Hier stellt sich die Frage hinsichtlich der Art und Weise einer zu erfolgenden „Identitätsprüfung“ im Rahmen einer Domainregistrierung. Insbesondere ob hierbei Verfahren wie das Postident Verfahren und das Videoident Verfahren in Erwägung gezogen werden. Fraglich ist bereits ob diese Verfahren überhaupt im Rahmen einer Domainregistrierung praktikabel sind und verhältnismäßig sind.

Einerseits besteht die Problematik, dass das bisherige schnelle und unkomplizierte Registrierungsverfahren durch die Identitätsprüfung komplizierter wird und andererseits die damit

verbundenen Kosten zu höheren Preisen und einer geringeren Attraktivität insgesamt führen können. Fraglich ist auch, ob eine Identifizierung im engeren Sinne notwendig ist, denn in der Regel ist bei der Registrierung eine existierende Bankverbindung anzugeben, so dass hierüber eine Rückverfolgbarkeit bzw. Auskunft über die Identität des Registrierenden möglich ist.

- Etablierung eines Notice and Action Verfahrens

eco befürwortet effektive Maßnahmen als Reaktion auf bekannt gewordene betrügerische Angebote. Im Zuge der weiteren Diskussionen und Beratungen sollte die Erfahrung der Internetwirtschaft zur Berücksichtigung kommen.

Für die Bewertung sowie die Anordnung einer Löschung bedarf es der Bestimmung einer zuständigen Stelle. Verpflichtete Unternehmen benötigen für das Löschen Rechtssicherheit. Nach Bestätigung eines Fake-Shops durch die zuständigen Strafverfolgungsbehörden die entsprechenden Maßnahmen gegenüber Hosting Providern, Registries und Registraren einleiten. Bei der Umsetzung der geplanten Maßnahmen zur Eindämmung von Fake-Shops muss der Grundsatz der Verhältnismäßigkeit ausnahmslos gewahrt werden.

Für den selbstverpflichtenden Einsatz eines „notice and action“ Verfahrens müssen angemessene und praktikable Umsetzungsbedingungen für Registries und Hoster vereinbart werden. Aktuell sehen sich die Registries und Hoster vor der Herausforderung, dass keine eindeutige Stelle bei den Ermittlungsbehörden oder bei Verbraucherzentralen benannt und eingerichtet ist. Es sollten eindeutige Kriterien sowohl für die Identifizierung von Fake-Shops als auch die Voraussetzungen für das Vorgehen festgelegt werden. Das Löschen und Sperren von identifizierten Fake-Shops sollte für Registries und Hoster nicht automatisch mit haftungsrechtlichen Problemstellungen einhergehen, wie sie auf Basis der aktuellen Rechts- und Vertragslage entstehen. Insbesondere dieser Punkt ist Hauptursache für das bisher restriktive Verhalten der Registries und Hoster im Umgang mit Fake Shops. Darüber hinaus sollte auf Basis einer Selbstverpflichtung bzw. einer späteren rechtlichen Verankerung eines „notice and action“ Verfahrens keine proaktiv geltende Pflicht zur stetigen Überwachung der angebotenen Infrastruktur auf die Registries oder Hoster ausgerollt werden.

Folgende Parameter sollten bei der weiteren Ausgestaltung eines auf selbstverpflichtender Basis eingeführten „notice and action“ Verfahrens Berücksichtigung finden und sichergestellt werden:

- Transparente und handhabbare Prüfkriterien, die eine eindeutige Bewertung und Identifizierung eines Angebots als Fake-Shop ermöglichen.
- Eine zuständige Stelle für die Bewertung und Anordnung, damit Anbieter rechtssicher Maßnahmen ergreifen können, ohne Haftungsrisiken ausgesetzt zu sein.
- Für den Shopbetreiber sollte es eine Möglichkeit geben, Entscheidungen zu beanstanden und eine Aufhebung der Klassifizierung als Fake-Shop zu erreichen.
- Zunächst sollte eine Kontaktaufnahme mit dem Hosting Provider erfolgen, da rechtswidrige Angebote auch gegen die Nutzungsbedingungen dieser Anbieter verstoßen dürften und eine Sperrung des Angebots rechtfertigen.

- Sodann kann an die Domainanbieter herangetreten werden, damit Domains suspendiert werden und nicht mehr „auflösen“.

- Flankierende Maßnahmen

Flankierend dazu wäre wichtig, Nutzer über die Gefahren von Fake-Shops aufzuklären, damit diese für Auffälligkeiten von unseriösen Shops sensibilisiert werden und nicht Opfer rechtswidriger Angebote werden. Listen von bestätigten Fake-Shops, die durch Nutzer eingesehen werden können, sind ebenfalls sinnvoll, wobei die Listen regelmäßig auf Aktualität geprüft werden müssten.

Listen bestätigter Fake-Shops sollten Anbietern nutzerautonomer Filtersysteme, Browseranbietern und Suchmaschinenbetreibern zur Verfügung gestellt werden, damit diese entsprechend ihre Nutzer auf rechtswidrige Angebote aufmerksam machen oder deren Aufruf unterbinden können.

Über eco:

Mit über 1.100 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Die Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie eine ethisch orientierte Digitalisierung bilden Schwerpunkte der Verbandsarbeit. eco setzt sich für ein freies, technikneutrales und leistungsstarkes Internet ein.