

## Domain protection – der Schutz vor Domainverlust.

*Wie Sie Ihre Domain gegen den unbeabsichtigten Verlust absichern.*

Domainnamen können durch ein unbeabsichtigtes Auslaufen der Registrierungsperiode, also einer fehlenden, bewusst nicht ausgeführten Verlängerung, verloren gehen. Eine weitere Gefahr stellt der Verlust durch Transferanträge Dritter dar, die entweder mit Entführungsabsicht (sog. Domain name hijacking), einer Schädigungsabsicht oder aus Spaß gestellt werden. Prominente Beispiele für die letzten beiden Fallvarianten sind für den Deutschen Namensraum ebay.de und google.de.

### 1. Angabe des tatsächlichen Inhabers

Lassen Sie sich immer als Inhaber der Domain eintragen. Lassen Sie nicht zu, dass sich Ihr Webmaster oder Webdesigner als Inhaber einträgt. Es gibt keinen Grund hier die Inhaberschaft abzuändern. Sofern eine juristische Person, also z.B. ein Unternehmen Inhaber sein soll, tragen Sie die korrekte Unternehmensbezeichnung einschließlich der Unternehmensform ein (z.B. united domains AG)

Sofern Sie Gründe haben, Ihre Identität nicht gegenüber Dritten preiszugeben, ist es notwendig sich über die Voraussetzungen in den verschiedenen Ländern und der jeweiligen Registry zu informieren. Eine Anonymisierungsdienst kann in Deutschland zum Verlust der Domain führen, wenn Dritten nicht klar ist, dass der Treuhänder tatsächlich als Treuhänder und nicht als nicht-berechtigter Inhaber auftritt. Zu den Voraussetzungen siehe das Urteil des BGH, grundke.de.

### 2. Aktualität der WHOIS Informationen / Korrekte Angaben / Admin-C:

Halten Sie die WHOIS-Daten Ihrer Domain ständig aktuell. Geben Sie dabei immer die korrekten Daten an, also beispielsweise die vollständige Bezeichnung der juristischen Person (united domains AG). Vermeiden Sie dabei die Angabe von Arbeitstiteln, Berufsbezeichnungen oder Namen von Organisationen, die keine juristische Person sind. Wenn Sie für eine derartige Domain später einen Inhaberwechsel oder Transferantrag stellen, stiften Angaben dieser Art nur Verwirrung und verzögern bestenfalls Ihren Auftrag.

Falls Ihr Provider oder die Vergabestelle sind kontaktieren, z.B. weil ein Dritter behauptet Sie würden seine Namens- oder Markenrechte verletzen und sie nicht erreichbar sind, kann dies zu einer Löschung Ihrer Domain führen (vgl. Section 3.7.7.2 ICANN Registrar Accreditation Agreement). Sofern Sie nicht im WHOIS stehen möchten, gibt es Alternativen, hier einen Treuhänder zu benennen.

Achten Sie darauf, den Admin-C ständig aktuell zu halten. Wenn Ihr Admin-C beispielsweise Ihr technischer Leiter ist und aus dem Unternehmen ausscheidet, ändern Sie davor die Person des Admin-C. Dieser ist z.B. bei .de Domains gegenüber der DENIC und in der Regel gegenüber Ihrem Provider befugt, über die Domain zu verfügen, also Inhaberwechsel und/oder Löschung durchzuführen, auch dann, wenn er im Innenverhältnis nicht dazu berechtigt ist oder entlassen wurde. Selbst bei Insolvenzen darf der Admin-C noch über die Domain verfügen, auch wenn der Inhaber sich bei einer derartigen Verfügung unter Umständen strafbar machen würde und zivilrechtlich nicht verfügungsberechtigt ist.

### 3. Sichere Zugangsdaten / Sichere Verwahrung Ihrer Zugangsdaten

Verwahren Sie Ihre Zugangsdaten für Ihr Kundenkonto stets vor dem Zugriff Dritter.

#### a) Zugangsberechtigter Personenkreis zu Ihren Domainsdaten

Halten Sie in einem geschäftlichen Umfeld den Kreis der Zugriffsberechtigten Personen auf die Administration Ihrer Domains begrenzt. Wählen Sie eine vertrauenswürdige Person aus, die

bestenfalls Ihr Unternehmen nicht nach kurzer Zeit wieder verlässt und in die Materie eingearbeitet ist.

#### **b) Sichere Verwahrung**

Speichern Sie Ihre Zugangsdaten nicht in Programmen wie Browsern oder Email-Clients ab. Durch Viren oder andere Schadprogramme können Dritte auf diese Daten Zugriff erhalten. Sofern Sie nicht um eine Speicherung umhinkommen, informieren Sie sich bitte über spezielle Software die für die Sicherung von Zugangsdaten geeignet ist.

#### **c) Sichere Zugangsdaten**

Wählen Sie bei der Auswahl von Login-Name und Passwort sichere Zeichenkombinationen, die nicht mit lexikalischen Begriffen identisch sind. Verwenden Sie dabei mindestens 7 Buchstaben, Sonderzeichen und Groß- und Kleinschreibung. Verwenden Sie für jeden Anbieter andere Login-Namen, zumindest aber unterschiedliche Passwörter.

#### **d) Sichere E-Mail Adresse**

Gegenüber Ihrem Domain Provider müssen Sie früher oder später eine E-Mail Adresse angeben. Verzichten Sie hier auf die Verwendung von Freemail Anbietern (Yahoo, Hotmail und Gmail). Diese Anbieter haben immer wieder mit Angriffen auf Ihre Postfächer zu kämpfen oder löschen Postfächer bei Inaktivität des Nutzers. Sobald diese Adresse wieder frei wird, kann ein Hacker diese Adresse registrieren und damit Ihre Post empfangen.

Vermeiden Sie es auch, eine Kontakt E-Mail Adresse zu verwenden, die zu einer Domain gehört, die bei Ihrem Provider liegt. Sollte der Zugang einmal gesperrt werden, kann Ihr Provider Sie mangels Angabe eine Adresse unter der Sie erreichbar sind, nicht kontaktieren. Die oben genannten generellen Anforderungen an die Sicherheit von Zugangsdaten sind natürlich auch auf die Zugangsdaten Ihres E-Mail Postfachs anzuwenden; auch wenn hier die Ausführen zum nicht speichern von Passwörtern in Programmen schwer durchzuhalten sind.

Falls Sie nicht umhinkommen, einen Freemail Anbieter auszuwählen, ändern Sie nach Erhalt Ihrer Zugangsdaten oder sonstiger sensibler Daten die E-Mail aus und löschen diese. Falls der Anbieter eine kostenpflichtige Upgrade-Möglichkeit bietet, die eine Löschung der Adresse bei längerer Inaktivität aufhebt, nutzen Sie diese!

Fügen Sie den Domainnamen und/oder die konkrete E-Mail Adress, mit denen Ihr Provider mit Ihnen korrespondiert zu einer Whitelist Ihres E-Mail Clients hinzu. So vermeiden Sie, dass wichtige Nachrichten nicht in Ihrem SPAM-Filter landen und Sie nicht erreichen. Achten Sie darauf, dass Ihr E-Mail Anbieter keinen SPAM-Filter einsetzt oder tragen Sie die Domain/E-Mail Adressen in die Whitelist Ihres E-Mail Providers ein (approved senders).

#### **e) Unterlassen Sie es, auf fragwürdige E-Mail zu antworten**

Sofern Sie vermeintlich E-Mails von Ihrem Provider/Registrar erhalten, unterlassen Sie es, diesem zu antworten oder auf Bilder/Links in der Email zu klicken. Vergewissern Sie sich gegebenenfalls bei Ihrem Provider, ob die E-mail tatsächlich von ihm stammt (vgl. Domain Scam: Chinesische Anbieter ...).

### **4. Auswahl des Registrars/Providers**

Informieren Sie sich über Ihren Provider. Welche Sicherheitsmaßnahmen bietet dieser für die Vermeidung von Domainverlusten an. Fragen Sie, ob Sie einen Sachbearbeiter zugeordnet werden können, mit dem Sie ausschließlich Kontakt haben und erläutern Sie ihm Ihre Nutzungsverhalten und Geschäftsmodell, damit auffällige Anfragen durch diesen erkannt werden.

## **5. Registrar-Lock**

### **a) Automatische Verlängerung Ihrer Domaininhaberschaft**

Falls Ihr Registrar nicht schon automatisch Ihre Domains für Sie verlängert, notieren Sie sich die Auslaufzeiten (expiration date) und verlängern Sie Ihre Domains rechtzeitig.

### **b) Halten Sie Ihren Domainbestand schriftlich fest**

Sofern Sie mit Ihrem Registrar nur per E-Mail oder Telefon in Kontakt treten, drucken Sie sich Registrierungsbestätigungsemails, Rechnungen und WHOIS-Auszüge aus. Einige Anbieter bieten auch den Export Ihrer Domainbestandsdaten mit Registrierungsinformationen an. Machen Sie von der Möglichkeit regelmäßig Gebrauch, wenn Sie über mehrere Domain verfügen. Bei einem Domainverlust werden Sie auf diese zurückgreifen müssen.

Ausführungen zur History der DENIC überlegen; Domaintools mit der History-Funktion; Impressum über die Waybackmaschine.

### **c) Unterlagen, die Sie indentifizieren**

Sofern möglich, hinterlegen Sie eine Kopie Ihres Geschäftspapiers bei Ihrem Anbieter, ggf. auch die Unterschriften der in Ihrem Unternehmens intern festgelegten Transferberechtigten, einschließlich des Admin-C.

### **d) Verzicht auf Erleichterungen für Transfers, Inhaberwechsel und Löschungen**

Verzichten Sie auf Tools Ihres Providers, die Transfers, Inhaberwechsel und Löschungen erleichtern, wenn Sie die Möglichkeit dazu haben.

### **e) Kontaktdaten Ihres Providers**

Erstellen Sie sich einen Aktionsplan bei drohendem Domainverlust. Notieren Sie sich hier die Kontaktdaten Ihres Providers und die Geschäftszeiten.

### **f) Nameserver, A-Records, MX-Einträge und Sicherheitskopien**

Halten Sie von den oben genannten Daten immer eine Kopie bereit, um die geschäftliche Operation absichern zu können. Ein falsch gesetzter MX oder A-Record kann für Ihr Unternehmen nicht nur peinlich, sondern auch geschäftsschädigend sein. Halten Sie für diesen Fall auch einen Aktionsplan bereit.

## **6. Versicherung**

Suchen Sie nach einer Versicherung, die Sie gegen den Verlust oder den Ausfall Ihrer Webpräsenz absichert. Fragen Sie gegebenenfalls Ihren derzeitigen Provider ob er gegen den Verlust von Domainnamen versichert ist und in welcher maximalen Höhe.

## **7. Einmaliger authInfo Code bei der Verwendung von EPP**

Stellen Sie sicher, dass Sie für jeden Domaintransfer und für jede Domain einen eigenen, einmaligen so genannten authInfo Code erhalten. Einige Anbieter nutzen nur einen Code für alle Domaintransfers eines Kunden, teilweise sogar für mehrere Kunden.

## **8. Benachrichtigung des Registranten bei Änderungen des Domainstatus**

Stellen Sie sicher, dass Sie bei Änderungen des Domainstatus (Transfer, Delete, Change of ownership) durch Ihren Registrar benachrichtigt werden. Beachten Sie in diesem Zusammenhang die Ausführungen zur Sicherheit Ihres E-Mailanbieters.