# Domain Integrity Guide 2024

Sichere Domain,
besser geschützte Marke

united domains

united-domains.de

Beim Thema Cyber Security wird ein wichtiger Aspekt oft übersehen: Prävention und Integrität auf Website- bzw. ganz konkret der Domain-Ebene.

MAXIMILIAN BURIANEK Online Brand Protection Strategist

# Wir möchten, dass Ihre Domains wirklich sicher sind

Die Digitalisierung wird durch technologischen Fortschritt, die Verlagerung von Kontakten und Kundenerfahrungen ins Internet sowie den Trend zu Remote-Working vorangetrieben. Für Unternehmen bedeutet das die Notwendigkeit, einerseits ihre digitale Präsenz zu erweitern, andererseits die Angriffsfläche für digitale Gefahren zu minimieren. Statistiken besagen, dass weltweit rund 90 Prozent aller Unternehmen von Cybercrime-Attacken betroffen sind.

Solche Attacken stellen Unternehmen vor große technische, organisatorische, juristische und finanzielle Herausforderungen. Für einen Großteil der Attacken registrieren und benutzen die Angreifer Domains, um Unternehmen und Marken zu schaden. Manche dieser Domains bestehen aus scheinbar willkürlich gewählten Zeichen oder Begriffen. Nicht selten ahmen die betrügerischen Domains aber die Markennamen derjenigen Unternehmen nach, die Ziel der Attacke sind. Bei der Einrichtung dieser Domains agieren die Angreifer in der Regel ungehindert und unbemerkt.

Warum ist das so? Zahlreiche Unternehmen verfolgen bis heute die defensive Strategie, wahrscheinliche und offensichtliche Domainvarianten präventiv zu registrieren, um die eigene Marke zu schützen. Doch die Methoden von Cyberkriminellen sind heute viel zu raffiniert, um Markendomains – also Domains, die den Markennamen beinhalten – mit diesem passiven Schutz ausreichend zu sichern.

Als Domain-Experten mit mehr als 20 Jahren Erfahrung möchten wir Ihnen mit dieser Praxis Guideline Insights aus der Praxis an die Hand geben, um Sie aktiv dabei zu unterstützen, Ihre Domains sicher zu machen. Machen Sie die Domain Integrität zu einem festen Bestandteil Ihrer Cyber Security-Strategie. Wir zeigen Ihnen, warum das notwendig ist und wie es funktioniert.

**Wir haben Ihnen unsere gebündelten Erkenntnisse zusammengestellt, damit Sie die Gefahren für Ihre Marke kennen – bevor Schaden entsteht. Diese Guideline vermittelt Ihnen ein essentielles Verständnis für Gefahren und geeignete Präventionsmaßnahmen, wie Sie Ihre Domains schützen. Es gibt mehr Möglichkeiten, als Sie denken – Prävention zahlt sich in jedem Fall aus.**

# Inhalt


1

## Technische Standards zum Schutz Ihrer Domains

Überprüfen Sie, ob Sie die Standards für Domainschutz umgesetzt haben

2

## Cyberkriminalität als Risiko für Markendomains

Prävention ist essenziell für effizienten Markenschutz

3

## Die Top-3-Bedrohungen für Domains

Phishing, Fake Shops und C-Level Impersonation

4

## Domains und Markenschutz

Effektive Domain-Strategien für Markeninhaber

5

## Wichtige Rechtsfälle und deren Urteile

Beispiele, die unterstreichen, wie wichtig umfassender Markenschutz ist

6

## Rechtliche Herausforderungen und Lösungen

Peter Müller, Fachanwalt für gewerblichen Rechtsschutz und Experte für Domain-Recht, im Interview

7

## Das united-domains Sicherheitskonzept

Schutzstrategie in drei Schritten

8

## Über united-domains

Wer wir sind, unsere Werte und Vision

# 1 Technische Standards zum Schutz Ihrer Domains

Domains sind nicht nur Adressen im Internet, sondern wesentliche IT-Assets, die einen signifikanten Wert für Ihr Unternehmen darstellen. Diese Perspektive erfordert ein umfassendes Verständnis der technischen Grundlagen, die für die Sicherung und Optimierung Ihrer Domains notwendig sind.

RINOR GASHI Online Brand Protection Strategist, united-domains GmbH

Die Domain ist eine Schlüsselressource, um eine globale Präsenz zu ermöglichen. Aber Domains sind auch einer Vielzahl von Risiken ausgesetzt. Voraussetzung für einen wirkungsvollen Schutz Ihrer Domains ist, dass Sie die Standards zu deren Schutz umgesetzt haben.

**Zwei-Faktor Authentifizierung (2FA)**
Die Implementierung von 2FA ist eine grundlegende Sicherheitsmaßnahme, um den Zugang zu Ihrem Domain-Management zu schützen. Reduzieren Sie das Risiko unbefugter Zugriffe durch einen zweiten, unabhängigen Nachweis Ihrer Identität, neben Ihrem Passwort.

**DDoS-Schutz**
Angesichts der Zunahme von Distributed Denial of Service (DDoS)-Angriffen ist ein wirksamer Schutzmechanismus gegen diese Art von Angriffen entscheidend. DDoS-Schutzmaßnahmen dienen dazu, Ihre Website verfügbar zu halten, selbst wenn sie Ziel eines koordinierten Angriffs wird, und sind somit essentiell für die Aufrechterhaltung Ihrer Online-Präsenz und -Dienste.

**DNSSEC**
(Domain Name System Security Extensions)
DNSSEC fügt eine zusätzliche Sicherheitsebene hinzu, indem es sicherstellt, dass die Besucher Ihrer Website tatsächlich zu der von Ihnen beabsichtigten IP-Adresse geleitet werden. Es schützt vor bestimmten Arten von Angriffen, die darauf abzielen, den Datenverkehr umzuleiten, und stellt sicher, dass die Datenintegrität zwischen den DNS-Servern und den Endnutzern gewahrt bleibt.

Jede dieser Technologien spielt eine entscheidende Rolle beim Schutz Ihrer Domains gegen eine Vielzahl von Bedrohungen, von der unerlaubten Übernahme bis hin zu Ausfallzeiten, die durch DDoS-Angriffe verursacht werden. Die Investition in diese Domain Table Stakes ist nicht nur eine Frage der technischen Anforderungen, sondern auch eine strategische Entscheidung, die die Widerstandsfähigkeit und Zuverlässigkeit Ihrer digitalen Assets stärkt.

**Betrachten Sie Ihre Domains als wertvolles IT-Asset und ergreifen Sicherheitsmaßnahmen. Dadurch bleibt Ihre digitale Präsenz zuverlässig, sicher und vertrauenswürdig. Ein entscheidender Schritt, um das digitale Rückgrat Ihres Unternehmens zu etablieren und zu festigen.**

Seit 1985 hat die Anzahl der registrierten Domains weltweit exponentiell zugenommen. Damals begann alles mit einer einzigen Domain, nordu.net. Heute spiegeln mehr als 366 Millionen registrierte Domains das Wachstum des Internets sowie die weltweite Präsenz von Unternehmen und Einzelpersonen wider. Dieser Anstieg bringt allerdings auch viele Gefahren mit sich – beispielsweise in Form von Cyberkriminalität.

## 1985

**Die erste Domain**
Die erste registrierte Domain, nordu.net, wurde 1985 erstellt. Dies markierte den Anfang der Domain-Ära und der Möglichkeit, Identitäten im aufstrebenden Internet zu etablieren.

## 1990

**Der .com-Boom**
In den 1990er-Jahren begann die Popularität von .com-Domains exponentiell zu steigen. Unternehmen und Einzelpersonen erkannten das Potenzial des Internets für Geschäft und Kommunikation.

## 2000

**Neue Endungen**
In den 2000er Jahren erfolgte die Einführung neuer Domain- Endungen wie .info, .biz und .name. Dies erweiterte die Auswahlmöglichkeiten für Domain-Namen erheblich. Um Markenrechtsstreitigkeiten rund um Domains effizient zu lösen, wurde 1999 das sogenannte UDRP Verfahren eingeführt.

## 2010

**gTLD-Ära**
In den Jahren nach 2010 wurden hunderte neuer generischer Top-Level-Domains (gTLDs) wie .app, .blog etc. eingeführt. Dies diversifizierte die Domain-Landschaft weiter und führte zu verstärkten Markenregistrierungen. Schutz der Markenidentität wurde zum neuen Thema.

## 2020

**Markenrisiken im Web3**
Ab 2020 gewannen Web3-Domains an Bedeutung und stellten das Markenrecht im digitalen Raum vor neue Herausforderungen. Web3-Domains nutzen Blockchain-Technologie, um dezentralisierte und benutzerkontrollierte Online-Identitäten zu ermöglichen.

## Soon

**Neue Trends**
Die Zukunft der Domains wird von Trends wie der Verbreitung von IPv6, verstärktem Fokus auf Sicherheit und der Integration von Domains in das Internet der Dinge (IoT) geprägt sein.

# 2 Cyberkriminalität als Risiko für Markendomains

Die Bedrohung von Markendomains (Domains, die den Markennamen beinhalten), z. B. durch Cybersquatting und Phishing, nimmt seit vielen Jahren kontinuierlich zu. Dieser Trend hat sich seit der coronabedingten Digitalisierung zusätzlich beschleunigt. Diese Bedrohung wird allerdings noch immer unterschätzt. Cyberkriminelle nutzen die dadurch vorhandene Angriffsfläche und die vermehrten Online-Aktivitäten aus, um ihre Angriffe zu intensivieren. Unternehmen sollten verstärkt auf Prävention von Cybersecurity auf Domainebene achten, um Schäden und hohe Kosten zu vermeiden.

Um sicherzustellen, dass Markennamen und geschützte Begriffe nicht von Dritten im Zusammenhang mit Domains missbraucht werden, müssen Gegenmaßnahmen getroffen werden. Die digitale Identität ist ein entscheidender Erfolgsfaktor von Unternehmen.

## Kunden

Schützen Sie Ihre Marke auf Domain-Ebene, um Ihre Kunden vor Gefahren zu bewahren. Oftmals setzen Dritte auf markenähnliche Domains, um Kunden auf betrügerische Websites zu locken. Das kann Ihren Ruf beeinträchtigen und Ihren Kunden erheblichen finanziellen Schaden zufügen.

## Online-Präsenz

Stellen Sie sicher, dass Ihre Marke einen einzigartigen und unverwechselbaren Markenauftritt transportiert.

## Rechtsstreitigkeiten

Schützen und beobachten Sie Ihre Domains – so lassen sich Kosten für Rechtsstreitigkeiten vermeiden oder minimieren.

**86,2**

Prozentsatz an Unternehmen, die 2021 von mindestens einem erfolgreichen Cyber-Angriff betroffen waren

Quelle: Cyberedge Group 2021 Cyberthreat Defense Report

**10,5**

Die Cyberkriminalität wird die Welt bis 2025 voraussichtlich 10,5 Billionen US-Dollar pro Jahr kosten.

Quelle: Forbes

**100.000**

Jeden Tag gibt es 100.000 neue bösartige Websites und 10.000 neue bösartige Dateien. Google hat im Januar 2021 über 2 Millionen Phishing-Websites identifziert, nach 1,7 Millionen im Januar 2020. Das entspricht einem Anstieg von 27 Prozent in nur zwölf Monaten. 2020 versuchten Angreifer auch von der Corona-Pandemie zu profitieren, und unterbrachen kritische Lieferketten. Angriffe auf Lieferketten nahmen in nur zwölf Monaten um 420 Prozent zu.

Quelle: retarus.com/blog/de/alarmierende

# 3 Die Top-3-Bedrohungen für Domains

## Phishing

Phishing ist eine betrügerische Methode, bei der Angreifer versuchen, persönliche Daten wie Passwörter, Kreditkarteninformationen oder andere vertrauliche Informationen zu stehlen. Cyberkriminelle nutzen Domains als Basis, um Phishing Angriffe durchzuführen, Malware zu verbreiten oder gefälschte Websites zu erstellen. Diese Angriffe können schwerwiegende Auswirkungen auf Ihr Unternehmen und Ihre Kunden haben.

## Fake-Shops

Dritte können Domains registrieren, die dem Namen Ihres Shops / Ihrer Marke ähneln, und diese zum Aufbau eines Fake-Shops verwenden. Kriminelle sind dabei fast immer in der Lage, sich eine URL zu sichern, mit der sie Nutzern vortäuschen, dass es sich um den originalen Shop handelt. Die Verbraucherzentrale schätzt, dass rund 4 Millionen Deutsche pro Jahr Opfer von Fake-Shops werden. Tendenz steigend.

## C-Level Impersonation

C-Level Impersonation bezeichnet Betrugsversuche, bei denen Angreifer sich als hochrangige Unternehmensmitarbeiter (wie CEO oder CFO) in E-Mails ausgeben, um sensible Informationen oder Geld zu erlangen.

# 4 Domains und Markenschutz

Um wirksame Strategien umzusetzen, ist ein unternehmensweites Bewusstsein für den Domainschutz essenziell.

CHRISTIAN DALLMAYER
Head of Marketing, united-domains GmbH

## Strategien

**Defensiv registrieren**
Registrieren Sie Domains, die Ihrer Marke ähnlich sind, oder Varianten Ihres Markennamens, die mit hoher Wahrscheinlichkeit versehentlich falsch geschrieben werden könnten. Dies verhindert, dass Dritte diese Domains nutzen, um Verwirrung zu stiften.

**Domain Monitoring**
Nutzen Sie Tools und Dienste zur Überwachung Ihrer Domains, um mögliche Markenrechtsverletzungen und Missbrauch frühzeitig zu erkennen. Wir beraten Sie hierzu gern.

**Rechtlicher Notfallplan**
Wenn Sie eine Markenrechtsverletzung feststellen, sollten Sie schnell handeln, um rechtliche Schritte einzuleiten und den Missbrauch zu stoppen.
Auch zu diesem Thema beraten wir Sie auf Wunsch.

**Interne Kommunikation**
Schulen Sie Ihr Team und Ihre Mitarbeiter hinsichtlich der Bedeutung des Markenschutzes auf Domainebene und die möglichen Risiken.

## Verantwortlichkeiten

Für einen effektiven Domainschutz müssen IT, Rechtsabteilung und Marketing zusammenarbeiten. Die IT-Abteilung registriert präventiv markenrelevante Domains, einschließlich typischer Tippfehler, unterstützt durch das Marketingteam. Sie kümmert sich um die Definition und Umsetzung der technischen Sicherheitsstandards rund um Domains. In vielen Unternehmen ist die IT-Abteilung auch zuständig für die Einrichtung eines Domain Monitorings, um eventuell gefährliche Domain-Registrierungen durch Dritte zu entdecken.

Die Rechtsabteilung definiert die Markenrechtsstrategie rund um Domains und bereitet einen Notfallplan für den Fall von Markenrechtsverletzungen vor. Zu den Aufgaben gehört insbesondere die Bestimmung wichtiger Begriffe, für welche Domains hinsichtlich des entsprechenden geistigen Eigentums gesichert werden sollen. Zudem prüft sie, inwiefern eigene Domains eventuell die Rechte anderer Markeninhaber verletzen.

Rechts- und IT-Abteilung arbeiten in vielen Fällen mit spezialisierten externen Domainanbietern zusammen, die sowohl bei technischen als auch rechtlichen Besonderheiten rund um Domains unterstützen.

Die Marketingabteilung schlägt zusätzliche Domainbegriffe für die Registrierung vor, beispielsweise für Kampagnen oder Produkte. Zudem bestimmt sie maßgeblich mit, welche Länderendungen auf Basis der relevanten Märkte registriert werden.

# 5 Wichtige Rechtsfälle und deren Urteile

Wie wichtig Markenschutz rund um die Domain ist, unterstreichen die nachfolgenden Beispiele.

## OpenAI: Der Fall ChatGPT.com

Im März 2023 leitete OpenAI ein UDRP-Verfahren zur Domain ChatGPT.com bei der WIPO ein, um den Domainnamen für seine beliebte KI-Chat-Plattform zu sichern. Zuvor wurde die Domain für die Webseite von ChatAI.com genutzt. Nachdem das Verfahren eingeleitet wurde, einigte sich OpenAI mit dem Eigentümer Site Matrix; seither leitet ChatGPT.com nun auf OpenAIs Webseite weiter. Was der Vergleich hinter der Einigung OpenAI gekostet hat, ist bisher nicht bekannt. Obwohl der Fall auf der WIPO-Website zum Zeitpunkt der Weiterleitung noch als aktiv geführt wird, zeigt die Weiterleitung, dass die Auseinandersetzung wohl beigelegt ist.

## Rekordfall: C. & J. Clark International

Ein weiteres bemerkenswertes Beispiel ist der Rekordfall von C. & J. Clark International, der zur Übertragung von 430 Domain-Namen führte. Der Fall verdeutlicht das Ausmaß, welches Domainrechtstreitigkeiten für ein einzelnes Unternehmen annehmen können. Fälle wie dieser illustrieren nicht nur die Komplexität des Domain-Namensrechts, sondern auch die zentrale Rolle, die Domain-Namen als geschäftskritische Assets spielen.

**Beschwerde:** Ursprünglich gegen 469 Domains, reduziert auf 429 nach Rückzug wegen ausgelaufener Registrierungen. **Domain-Typen:** Verschiedene Schemata, inklusive Länder-/Städtenamen und Variationen ohne „s“. **Inhalt:** Meist Shops, die Clark’s Schuhe und andere Marken anbieten. **Verfahrensdauer:** Länger als üblich, Einreichung am 7. Juli 2023, mehrfache Änderungen erforderlich. **Entscheidung:** Matthew Kennedy entschied fast vollständig zugunsten von Clark’s, außer für shopclarksshoe.com. **Begründung:** Zusammenhang zwischen Domains durch Registrierung, IP-Adressen und Stores. Englisch als Verfahrenssprache zur Kostenminimierung. Markenähnlichkeit, Fehlen von Rechten/Interessen der Gegner, Bösgläubigkeit bestätigt für 428 Domains. **Ergebnis:** Transfer von 428 Domains an Clark’s bestätigt, Beschwerde für shopclarksshoe.com abgewiesen, kein Einfluss auf zukünftige Verfahren.

## AVM

Am 22. Januar 2024 wurde die Domain „fritz.box“ von einer unbekannten Person registriert und präsentierte eine NFT-Werbeseite, anstatt der erwarteten Router-Verwaltung. Für Besitzer von AVM-Routern stellte dies ein besonderes Risiko dar, da die Domain „fritz.box“ standardmäßig für die Verwaltung der Router im heimischen Netzwerk verwendet wird. Nutzer, die die Domain außerhalb ihres Heimnetzwerks aufriefen, könnten leicht Opfer von Phishing-Angriffen werden, indem sie auf gefälschte Login-Seiten gelangen und ihre Zugangsdaten preisgeben.

AVM startete am 15. Februar ein Verfahren nach der Uniform Domain-Name Dispute-Resolution Policy (UDRP) vor der World Intellectual Property Organization (WIPO), um die Domain zurückzuerlangen, da sie ihre Markenrechte verletzte. Der Domaininhaber bot die Domain auf der NFT-Plattform Opensea für 420 ETH (ca. US$ 1 Mio.) zum Verkauf an.

Das dreiköpfige Panel der WIPO bestätigte die Beschwerde von AVM und entschied auf Übertragung der Domain an AVM. Das Panel stellte fest, dass der Domaininhaber kein berechtigtes Interesse an der Domain hatte und sie in böser Absicht registriert wurde.

Dieser Fall unterstreicht die Notwendigkeit einer umfassenden Marken- und Domainstrategie, um sich vor Cybersquatting zu schützen. AVM empfiehlt Fritzbox-Besitzern, zur sicheren Nutzung die IP-Adresse des Routers zu verwenden.

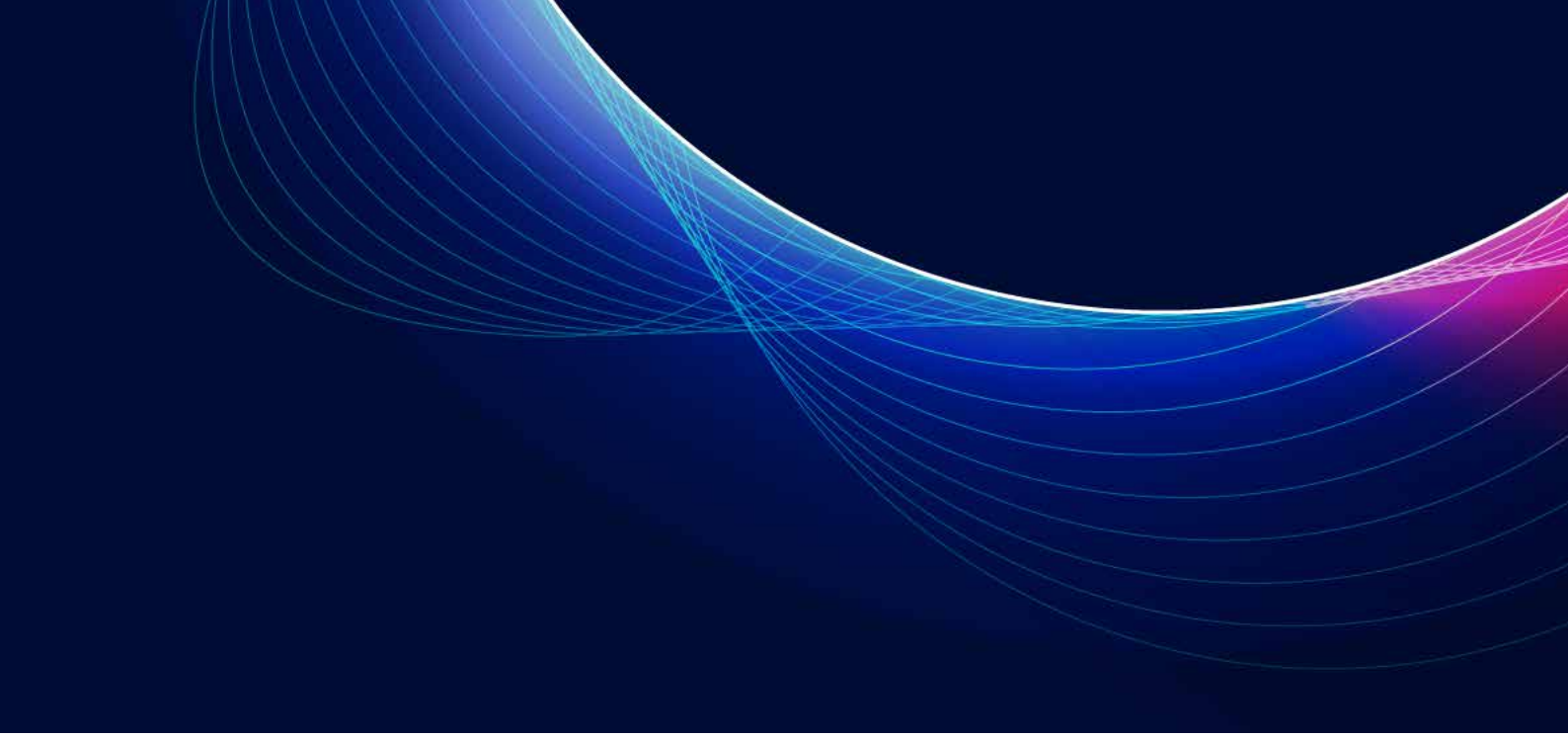
# IBM

In einem kürzlich durchgeführten UDRP-Verfahren, welches vom WIPO Arbitration and Mediation Center verhandelt wurde, standen die International Business Machines Corporation (IBM), USA, und Red Hat, Inc., USA, dem Angeklagten Registration Private, Domains By Proxy, LLC, USA / Terry McGlynn, einer Person, die im Bereich der Verkaufsstrategien für Cloud-Technologien tätig ist, gegenüber. Im Mittelpunkt der Auseinandersetzung standen eine Vielzahl von Domain-Namen, die Markennamen von IBM und Red Hat enthielten und ohne Zustimmung der Kläger registriert wurden. Der Fall wurde unter der Nummer D2023-1485 geführt und zeichnete sich durch eine komplexe Sachlage und mehrere juristische Herausforderungen aus.

**Die wichtigsten Fakten des Verfahrens sind wie folgt zusammengefasst:**

**Die Parteien:** Die Kläger in diesem Rechtsstreit waren die International Business Machines Corporation (IBM) und Red Hat, Inc., beide US-amerikanische Unternehmen. **Die strittigen Domain-Namen:** Im Zentrum des Streits standen mehrere Domain-Namen, die die Markennamen IBM und Red Hat enthielten. Diese Domains waren bei verschiedenen Registraren wie 1API GmbH und GoDaddy.com, LLC registriert. **Prozessgeschichte:** Die Beschwerde wurde am 4. April 2023 beim WIPO Arbitration and Mediation Center eingereicht. Nach der formalen Prüfung und der Benachrichtigung der Beklagten begann das Verfahren am 28. April 2023. Eine Antwort des Beklagten wurde rechtzeitig eingereicht. **Faktischer Hintergrund:** IBM ist ein renommiertes Technologieunternehmen. Red Hat bietet Open-Source-Internetinfrastrukturlösungen an. **Inhaltliche Argumentation der Parteien:** Die Kläger argumentierten, dass die Domain-Namen ihren Marken verwirrend ähnlich seien und der Beklagte keine Rechte oder legitimen Interessen an den Namen habe. Sie behaupteten weiterhin, dass die Domain-Namen böswillig registriert und genutzt wurden. **Diskussion und Feststellungen:** Das Schiedsgericht stellte fest, dass die Domain-Namen den Marken IBM und RED HAT ähnlich sind und der Beklagte keine Rechte oder legitimen Interessen an ihnen hat. Zudem wurde entschieden, dass die Domains böswillig registriert und genutzt wurden. **Entscheidung:** Das Schiedsgericht ordnete die Übertragung der strittigen Domain-Namen an die Kläger an.

**Diese und viele weitere Fälle unterstreichen, wie wichtig es ist, seine Online-Markenrechten zu schützen und wie sich Unternehmen gegen die unbefugte Nutzung und Registrierung von Domain-Namen verteidigen können.**



# 6 Rechtliche Herausforderungen und Lösungen

Unternehmen müssen sich damit auseinander setzen, wie sie potenziell schädliche Domains für ihre Marken identifizieren. Im Falle einer Markenrechtsverletzung sollten Unternehmen schnell handeln und effektive Gegenmaßnahmen ergreifen. Dazu zählen sowohl die Kontaktaufnahme mit dem jeweiligen Domainregistrar als auch rechtliche Verfahren sowie Ankaufversuche. Die Durchführung der Gegenmaßnahmen, insbes. der rechtlichen Schritte, können zeitaufwendig sein, sind jedoch essenziell, um die Rechte eines Unternehmens zu wahren und dessen Reputation zu schützen.

Um Herausforderungen wie den Markenmissbrauch durch Domainregistrierungen zu bewältigen, ist ein proaktiver Ansatz unerlässlich. Unternehmen sollten relevante Domains im Voraus registrieren, um Missbrauch zu verhindern. Im Falle einer Rechtsverletzung können internationale Schlichtungsverfahren wie die Uniform Domain-Name Dispute-Resolution Policy (UDRP) genutzt werden, um effektiv gegen unzulässige Domainregistrierungen vorzugehen. Dies erfordert eine enge Zusammenarbeit zwischen IT-Experten und Rechtsabteilungen, um sowohl technische als auch rechtliche Strategien zu integrieren.

**Lesen Sie im nachfolgenden Interview mit Peter Müller, Fachanwalt für gewerblichen Rechtsschutz und Experte für Domain-Recht, wie Unternehmen ihre Domain effektiv schützen können.**

# Experten-Interview

Letztlich ist es entscheidend, dass Unternehmen sowohl technologisch als auch rechtlich gut aufgestellt sind, um sich gegen Markenrechtsverletzungen im digitalen Raum effektiv zu wehren.

PETER MÜLLER Rechtsanwalt, PM-Legal

**Was sind die größten Herausforderungen im Bereich des Domainrechts?**

Die IT-Welt sieht sich mit einer Vielzahl von Herausforderungen konfrontiert, wobei Cyberangriffe, die Domains als Einfallstore nutzen, besonders hervorstechen. Phishing, Malware und die Einrichtung von Fake Shops auf Domains, die etablierten Marken ähneln, sind nur einige Beispiele. Diese Bedrohungen betreffen nicht nur die IT-Infrastruktur, sondern auch die Markenintegrität. Daher ist ein umfassender Multi-Stakeholder-Ansatz erforderlich, der sowohl technische als auch rechtliche Aspekte berücksichtigt.

**Wie können Unternehmen ihre Domain absichern?**

Die Sicherung einer Domain ist nicht nur eine technische, sondern auch eine rechtliche Herausforderung. Es beginnt mit der Sicherstellung, dass die eigenen Domains und die damit verbundenen Markenrechte geschützt sind. Dies erfordert eine sorgfältige Überwachung und Verwaltung aller registrierten Domains eines Unternehmens.

Zudem ist es wichtig, relevante Haupt- und Zusatzdomains zu registrieren, um Cybersquatting und verwandte Aktivitäten zu verhindern. Die rechtlichen Herausforderungen sind umfangreich und erfordern eine enge Zusammenarbeit zwischen IT- und Rechtsabteilungen.

**Was können Unternehmen gegen markenrechtsverletzende Domains unternehmen?**

Die Lösungen für rechtliche Herausforderungen im Bereich markenrechtsverletzender Domains sind vielschichtig. Zunächst ist eine proaktive Strategie zur Identifizierung und Dokumentation aller Domains, die einem Unternehmen gehören, unerlässlich. Im Falle einer Markenrechtsverletzung können Unternehmen auf juristische Mittel wie Unterlassungs- und Schadensersatzklagen zurückgreifen. Zudem sind internationale Vereinbarungen wie die Uniform Domain-Name Dispute- Resolution Policy (UDRP) hilfreich, um gegen unzulässige Domainregistrierungen vorzugehen. Letztendlich ist eine Kombination aus technischen Sicherheitsmaßnahmen und einer soliden rechtlichen Strategie der Schlüssel zum Schutz vor Markenrechtsverletzungen.

# 7 Das united-domains Sicherheitskonzept für Ihre Domains

## Präventive Maßnahmen

Wir unterstützen Sie bei Ihrer Domain-Strategie, um zu definieren, welche Domains für Ihre Ziele und Zielgruppen wichtig sind – und auf welche Sie verzichten können (Domain-Inventur). Bei united-domains können Sie mehr als 1.000 Domain-Endungen registrieren – die Voraussetzung für international ausgerichtete Markenstrategien.

→ Zum kostenfreien Beratungsgespräch

## Domain-Monitoring

Mit unserer intelligenten Lösung für automatisiertes Domain-Monitoring überwachen Sie bestehende und neue Domainregistrierungen, die Ihre Marke oder ähnliche Begriffe enthalten. Das Domain-Monitoring erkennt missbräuchliche Domainregistrierungen, die für Phishing, Spam oder den Verkauf von gefälschten Plagiaten über Fakeshops genutzt werden könnten.

→ Zum Domain-Monitoring

## Support beim Durchsetzen von Rechten

Durch unsere Partnerschaft mit spezialisierten Rechtsexperten können Maßnahmen gegen markenrechtsverletzende Domains schnell umgesetzt werden. Unsere Partner haben umfangreiche Erfahrung, um Ihre Marke durch Website Takedowns, Unterlassungserklärungen und Streitbeilegungsverfahren effektiv zu schützen.

→ Zum kostenfreien Beratungsgespräch

# 8 Über uns

united-domains GmbH ist ein etablierter Domain-Registrar und Anbieter von Webhosting-Diensten. Mit Sitz in Deutschland bieten wir professionelle Lösungen für Domainregistrierung, Web-Präsenz-Management und sichere Markendomains. Zu unseren Kunden gehören viele der bekanntesten Marken. Diese schätzen unsere Domainexpertise, unsere hohen technischen Standards sowie den united-domains Kundenservice, der Unternehmen auch bei komplexen Domainanforderungen stets zuverlässig weiterhilft.

## Wer wir sind

united-domains wurde im Jahr 2000 gegründet und ist seitdem ein führender Domain-Registrar in Deutschland. Mit über 1,6 Millionen verwalteten Domains sind wir ein vertrauenswürdiger Dienstleister für über 300.000 Kunden weltweit. Unser USP ist unser erstklassiger Kundenservice in Kombination mit innovativen, intuitiven Technologien.

## Was wir tun

Unser Service umfasst alles rund um das Registrieren und Management von Internetdomains sowie Hosting- und Security-Lösungen für Websites. Darüber hinaus unterstützen wir Kunden bei Online-Markenschutzstrategien und bieten zahlreiche Services rund um Webpräsenzmanagement an.

## Unsere Vision

Wir helfen, eine sichere digitale Welt zu bauen, indem wir starke digitale Identitäten ermöglichen. Für dieses Ziel unterstützen wir Professionals, Startups und große Unternehmen dabei, ihre digitale Identität zu entwickeln, Marken online zu etablieren und zu schützen. Unser Anspruch ist, bei dieser Aufgabe der beste Technologiepartner für unsere Kunden zu sein.

## Unsere Mission

Die Zufriedenheit unserer Kunden ist unser Nordstern. Dafür bieten wir Ihnen drei wesentliche Vorteile: die größte Auswahl an Domains, intuitive Lösungen, die wir basierend auf Ihren Bedürfnissen stetig weiterentwickeln und erstklassigen Kundenservice und Beratung durch unsere Experten.

## Unsere Werte

**KUNDENZENTRIERT** Unsere Kunden stehen im Mittelpunkt – ohne Kompromisse. Denn Domains und Hosting sind ein komplexes Thema, bei dem wir laufend auf sich ändernde Kundenbedürfnisse reagieren. Stetige Optimierungen und beste Beratung sind uns ein Anliegen.

**VERTRAUENSWÜRDIG** Die digitale Identität unserer Kunden gehört zu den wertvollsten Grundlagen ihres Unternehmenserfolgs. Deshalb genießen Sicherheit, Zuverlässigkeit und Vertrauen bei uns oberste Priorität.

**PROAKTIV** Wir reagieren nicht nur auf die Bedürfnisse unserer Kunden, wir gehen einen Schritt weiter: wir informieren unsere Kunden proaktiv und kommunizieren stets transparent und vorausschauend.

Sie haben Fragen rund um den Schutz Ihrer Markendomains? Sprechen Sie uns an, unsere Experten beraten Sie gerne persönlich.

**Rinor Gashi**
**Online Brand Protection Strategist**
Telefon 08151 36867-40
brands@united-domains.de