CSC

Der „IP Frontiers Report“ 2025

Proaktive Sicherheitsstrategien gegen IP-Rechtsverletzungen

Einführung: Eine sich schnell verändernde, risikoreiche Welt

Der Ruf eines Unternehmens ist eng mit seiner Online-Präsenz verknüpft. Betrügerischen Akteuren bietet sich hier die Gelegenheit, bekannte Marken zu missbrauchen – sei es durch die Einrichtung irreführender Websites, das Kopieren von Produkten oder Logos oder die Erstellung gefälschter Social-Media-Profile, die die jeweilige Marke kopieren.

Mittlerweile sehen sich betrügerische Akteure mit deutlich geringeren Hürden konfrontiert, sodass Rechtsverletzungen gegen das geistige Eigentum (IP) einfacher denn je zu begehen sind. IP-Rechtsverletzungen sind immer schwieriger zu erkennen und nachzuverfolgen, und die böswilligen Akteure lassen sich mit Unterlassungsaufforderungen allein oft nicht in ihre Schranken weisen.

Angesichts dieser Herausforderungen profitieren Unternehmen davon, eine Reihe von Maßnahmen zu ergreifen, um die Durchsetzung ihrer IP-Rechte zu stärken und ihre Marken, Urheberrechte und sonstigen Rechte an geistigem Eigentum zu schützen.

Wie sollten Rechtsabteilungen in einem Umfeld knapper werdender Ressourcen enger mit Marketing-, IT- und Sicherheitsteams zusammenarbeiten, um Maßnahmen zum Schutz geistigen Eigentums zu priorisieren und sicherzustellen, dass Budgets sinnvoll eingesetzt werden?

Betrügerischen Akteuren gelingt es immer häufiger, Rechtsverletzungen gegen das geistige Eigentum zu begehen. Daher ist es für alle von Vorteil, sich der Situation bewusster zu werden, sich stärker auf Technologie zu konzentrieren und eine engere Zusammenarbeit zwischen den mit Domains befassten Teams zu fördern, sagt Ian McConnel, Chief Legal Officer bei CSC. „Ob es uns gefällt oder nicht, Domain-Management ist ein zentraler Bestandteil von Cybersicherheitsstrategien, nicht nur, wenn es um den Schutz der wertvollsten Domainnamen geht."

UNSERE EXPERT:INNEN

Ian McConnel
CSC Chief Legal Officer

Ihab Shraim
Chief Technology Officer,CSC Digital Brand Services

Elliott Champion
CSC Global Product Director,Brand Protection and Anti-Fraud

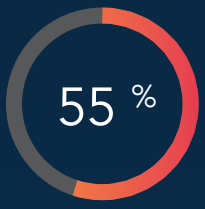
Mary Jo Murphy
CSC Product Manager,Brand and Fraud Services

Unsere wichtigsten Forschungserkenntnisse

Wir haben im zweiten Quartal 2025 300 erfahrene Juristen und Juristinnen befragt und Folgendes festgestellt:

Die Zahl der Online-IP-Rechtsverletzungen nimmt zu und wird voraussichtlich weiter steigen

Die überwiegende Mehrheit der Befragten (91 %) gab an, dass sie angesichts der zunehmenden Bedrohung durch Online-IP-Rechtsverletzungen beunruhigt sind.



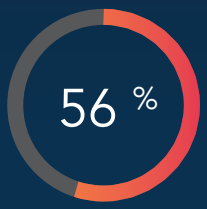
Mehr als die Hälfte (55 %) gab an, dass sie in den nächsten drei Jahren mit einem deutlichen Anstieg der Online-IP-Rechtsverletzungen rechnen.

Laut den Befragten traten die folgenden drei Arten von Online-IP-Rechtsverletzungen am häufigsten auf:

KI spielt eine wichtige Rolle bei der Zunahme von IP-Rechtsverletzungen

Eine Mehrheit (88 %) gab an, dass KI-gestützte Systeme zu einer Zunahme von Rechtsverletzungen führen.

Die Befragten sind sich der Vorteile einer Auslagerung der Überwachung von Online-IP-Rechtsverletzungen bewusst



Mehr als die Hälfte (56 %) gab an, derzeit bestimmte Maßnahmen zur Überwachung von Online-IP-Rechtsverletzungen auszulagern, aber aktiv nach Möglichkeiten zu suchen, weitere Aufgaben auszulagern.

Die meisten Rechtsabteilungen arbeiten bereits mit IT- und Sicherheitsteams zusammen, um die Risiken von IP-Rechtsverletzungen besser zu verstehen

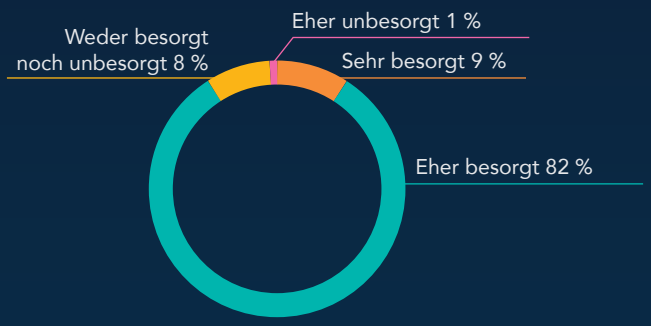
Fast zwei Drittel (64 %) bewerteten ihre Zusammenarbeit mit Kollegen und Kolleginnen aus dem Bereich IT-Sicherheit als gut (vier von fünf Punkten), **während weitere 22 %** angaben, dass sie sehr eng mit ihrem IT-Sicherheitsteam zusammenarbeiten.

Die Zahl der IP-Rechtsverletzungen steigt weiter an

In den letzten Jahren sind mehrere Faktoren zusammengekommen, die sich tiefgreifend auf das Ausmaß der IP-Rechtsverletzungen ausgewirkt haben.

Zu diesen vielfältigen Treibern zählen die zunehmende Verbreitung von Crimeware-as-a-Service-Kits (CaaS), der anhaltende Anstieg der Lebenshaltungskosten und das kontinuierliche Wachstum des Online-Shoppings – allesamt Faktoren, die Rechtsverletzungen gegen das geistige Eigentumsrecht begünstigen und damit den Ruf von Unternehmen schädigen und deren Profit schmälern.

Bemerkenswert ist, dass mehr als 90 % der Befragten im Rahmen der weltweiten Umfrage von CSC angaben, dass sie angesichts der Gefahr von Online-IP-Rechtsverletzungen gegen Unternehmen wie das ihre besorgt seien.



Ein Viertel gab an, in den letzten 12 Monaten einen „signifikanten“ Anstieg der Online-IP-Rechtsverletzungen verzeichnet zu haben; rund ein Drittel (35 %) gab an, in den letzten drei Jahren einen „signifikanten“ Anstieg verzeichnet zu haben.

Laut der Befragten sind die drei am häufigsten missbrauchten Vermögenswerte:

- Internetinhalte oder Markeninhalte (genannt von 45 %)
- Mobile Apps (30 %)
- Online-Marktplätze (17 %)

„Verbraucher:innen sind immer auf der Suche nach günstigeren Produkten, beispielsweise Arzneimitteln, Autoteilen und Konsumgütern – und böswillige Akteure machen sich dies zunutze“, so Mary Jo Murphy, CSC Product Manager, Brand and Fraud Services

Mit Blick auf die Zukunft gaben die meisten Befragten (89 %) an, dass sie in den nächsten drei Jahren einen Anstieg der IP-Rechtsverletzungen erwarten. Neun von zehn Befragten (90 %) erwarten ebenfalls eine Zunahme in den nächsten 12 Monaten.

Welche der folgenden Arten von Online-IP-Rechtsverletzungen machen Ihrem Unternehmen am meisten Sorgen?

- Fälschung
- Markenmissbrauch
- Identitätsdiebstahl
- Designrechtsmissbrauch
- Urheberrechtsmissbrauch

„Welche Bedeutung diese Art von Rechtsverletzungen für Sie haben, hängt von Ihrer Perspektive ab“, fügt Ian hinzu. „Als verbraucherorientiertes Unternehmen würde ich mir vor allem Sorgen um Produktfälschungen machen, als Finanzdienstleister hingegen eher darum, dass betrügerische Akteure Markenzeichen missbrauchen, um Phishing- oder Cyberangriffe auf Kunden und Kundinnen zu ermöglichen.“

> Ihre Reputation wird durch Ihre Online-Präsenz repräsentiert. Das bedeutet, dass Sie Ihre Reputation heute anders schützen müssen als in der Vergangenheit. Es gibt eine massive Zunahme von Bedrohungsvektoren, die auf Unternehmen abzielen, und die einfachsten Ziele für Angriffe sind Domainnamen und IP-Adressen. Der Unterschied zu früher besteht darin, dass betrügerische Akteure einst Hunderttausende von Phishing-E-Mails verschickten, in der Hoffnung, dass 2 % oder 3 % der Empfänger darauf reagieren würden, während betrügerische Aktivitäten heutzutage zielgerichteter sind und eine viel höhere Erfolgsquote aufweisen.
>
> **– Ihab Shraim, Chief Technology Officer, CSC Digital Brand Services**

DESHALB IST DER SCHUTZ VON DOMAINNAMEN IM KAMPF GEGEN IP-DIEBSTAHL WICHTIG

„Domainnamen sind ein zentraler Bestandteil der täglichen Interaktion und Kommunikation zwischen Menschen. Es ist so alltäglich, dass die Menschen gar nicht merken, dass sie mit einem Domainnamen interagieren, und es für selbstverständlich halten, dass sie unbeschadet bleiben. Dennoch sind gefälschte Web-Domainnamen oft der Ausgangspunkt für schwerwiegende IP-Rechtsverletzungen, und für betrügerische Akteure war es noch nie so einfach, einen beliebigen Domainnamen zu registrieren“, so Elliott Champion, CSC Global Product Director, Brand Protection and Anti-Fraud.

„Ist Ihnen aufgefallen, dass man in manchen Restaurants mittlerweile einen QR-Code zum Bestellen verwendet? Beim Scannen wird man direkt zu einer Domain weitergeleitet, ohne zu wissen, wohin diese eigentlich führt – man vertraut der Sache einfach“, erklärt Elliot. „Das zeigt, wie wichtig Domainnamen für das tägliche digitale Erlebnis sind. Wir alle vertrauen ihnen und interagieren mit ihnen, obwohl es nur wenige Minuten dauert, einen gefälschten Namen einzurichten. Das bedeutet, dass die Eintrittsbarrieren für diese Art von betrügerischen Aktivitäten mittlerweile unglaublich niedrig sind.“

KI spielt eine immer wichtigere Rolle bei IP-Rechtsverletzungen

In kürzester Zeit ist KI in den Mittelpunkt der globalen Geschäfts- und Produktivitätsdiskussion gerückt. Die Kehrseite der Medaille ist jedoch, dass KI aus Sicht der Betrugsbekämpfung und Risikominimierung bereits dazu eingesetzt wird, äußerst realistische und komplexe IP-Assets wie Logos, Bilder und Unternehmensinhalte zu erstellen. Angesichts der zunehmenden Verbreitung von KI und KI-gestützten Funktionen besteht für Rechtsabteilungen die große Herausforderung darin, Risiken bestmöglich zu erkennen und der Entwicklung einen Schritt voraus zu sein.

Es überrascht nicht, dass etwa neun von zehn Befragten (88 %) unserer Umfrage angaben, dass KI-fähige Systeme für einen Anstieg der Häufigkeit von Vorfällen verantwortlich sind.

Die Mehrheit der Befragten (93 %) gab außerdem an, dass sie angesichts der Möglichkeit, mithilfe von KI gefälschte Assets zu erstellen, erhebliche Auswirkungen auf ihr Geschäft befürchten.

„Heutzutage ist es ein Kinderspiel, ein KI-gestütztes Tool zu nutzen, um fiktive Inhalte zu erstellen, die sich sehr leicht verwerten lassen“, sagt Ian. „Die Zeiten, in denen man sich hinsetzen und eine Reihe gefälschter Webseiten programmieren musste, sind vorbei. Mit der zunehmenden Komplexität der Tools werden auch die Möglichkeiten für weniger technisch versierte betrügerische Akteure weiter zunehmen. „Betrügerischen Akteuren sind nur durch ihre Vorstellungskraft Grenzen gesetzt.“

Unternehmen stehen vor neuen und sich ständig weiterentwickelnden KI-bedingten Herausforderungen. Neun von zehn Befragten gaben außerdem an, dass sie befürchten, KI-Tools könnten die Daten oder das geistige Eigentum ihres Unternehmens zum Trainieren von Modellen verwenden und so Inhalte generieren, die von Wettbewerbern genutzt werden könnten. Die Mehrheit der Befragten, die dies befürchten, ist jedoch der Meinung, angemessene Schutzmaßnahmen getroffen zu haben.

Als positives Zeichen ist zu werten, dass viele Unternehmen die zunehmende Bedrohung durch KI erkennen und ihre Abwehrmaßnahmen durch interne Schulungsprogramme und andere Initiativen verstärken.

Fast 70 % der Befragten bewerten die Qualität der internen Richtlinien oder Vorgaben ihres Unternehmens für den Einsatz von KI bei der Erstellung von geistigem Eigentum als gut, während 20 % diese als ausgezeichnet bewerten.

Künftig werden Schulungen wahrscheinlich eine immer wichtigere Rolle bei der Prävention von KI-bedingten Risiken in Unternehmen spielen.

DIE UNTERSCHEIDUNG ZWISCHEN FAKTEN UND FIKTION WIRD IMMER SCHWIERIGER

Eines der drei größten Probleme für die Befragten im Zusammenhang mit IP-Rechtsverletzungen ist Identitätsdiebstahl, darunter realistische KI-generierte Darstellungen von Führungskräften, die dazu missbraucht werden können, um Mitarbeiter:innen um finanzielle Zuwendungen zu bitten.

„Es gibt genug Inhalte von CEOs, darunter Reden, Beiträge und Videomaterial, mit denen betrügerische Akteure innerhalb weniger Stunden KI-Darstellungen erstellen können, die viele Menschen in einem Unternehmen täuschen würden“, so Ian. „Irgendwann werden wir eine Online-Darstellung von jemandem sehen, die genau wie die Person aussieht, mit der wir regelmäßig interagieren, und wir werden nicht in der Lage sein, Wahrheit und Fiktion voneinander zu unterscheiden.“

„Bisher ist das noch nicht der Fall, da gefälschte Video-Chats noch etwas unnatürlich wirken. Aber die Technologie verändert sich so schnell und verbessert sich exponentiell, dass es ehrlich gesagt nur eine Frage der Zeit ist.“

„Das bedeutet, dass Unternehmen Prozesse und Systeme einrichten müssen, die sich hinsichtlich der Authentifizierung der Kommunikation – sei es per Telefon, Video oder E-Mail – nicht ausschließlich auf den Einzelnen verlassen. In fünf Jahren wird es keine Schulungen mehr geben, die diese betrügerischen Praktiken verhindern können.“

„Gegenmaßnahmen beginnen damit, Domainnamen zu sperren, über die derartige Kommunikationsformen eingeleitet werden können, und geeignete Protokolle einzurichten, um die Herkunft illegaler Kommunikation zu überprüfen.“

Die Budgets wachsen, aber nicht immer werden Ausgaben priorisiert

Wie haben sich dedizierte IT-Budgets angesichts der zunehmenden Anzahl und Vielfalt von Risiken und Katalysatoren verändert, um dieser Herausforderung gerecht zu werden?

Unsere Studie ergab, dass die Budgets für IP-Rechtsverletzungen und Markenschutz steigen: Zwei Drittel (67 %) der Befragten gaben an, dass sie in den nächsten drei Jahren einen „signifikanten“ Anstieg erwarten, während knapp die Hälfte (46 %) einen „signifikanten“ Anstieg für das kommende Jahr prognostiziert.

In den nächsten 12 Monaten erwarten die Befragten zusätzliche Investitionen in folgenden Bereichen:

72 %	69 %	68 %
Interne Technologie	Höhere Mitarbeiterzahl im IP-Management-Team	Mitarbeiterzuwachs in der gesamten Rechtsabteilung

Fast die Hälfte (44 %) erwartet ein stärkeres Outsourcing an dedizierte IP-Spezialisten wie CSC.

Diese steigenden Investitionen werfen eine wichtige Frage auf: Wohin sollten die Ressourcen gelenkt werden, um die größte Wirkung zu erzielen? Anstatt zu versuchen, jeden potenziellen Kanal oder jede Variante eines Domainnamens abzusichern, sollten Unternehmen ihre Ausgaben dort priorisieren, wo sie die größte Wirkung erzielen.

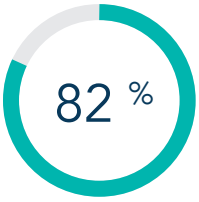
„Es geht nicht nur darum, die Budgets zu erhöhen, sondern auch darum, wie sie eingesetzt werden”, so Ian. „Wie viel geben Sie aus, um in Sachen KI auf dem neuesten Stand zu sein? Wie viel geben Sie aus, um die richtigen Ressourcen für eine angemessene Risikominderung bereitzustellen?“

Aufgrund des raschen Aufkommens neuer Risiken und der wachsenden Zahl von Kanälen, über die Rechtsverletzungen gegen das geistige Eigentum begangen werden, kann die Risikominderung nicht einmalig erfolgen, sondern erfordert eine kontinuierliche Analyse und Überwachung. Immer öfter wenden sich Unternehmen an externe Partner, um diese Herausforderung zu bewältigen.

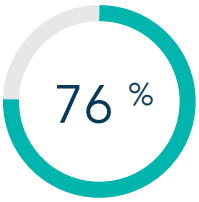
> Die Plattformen verändern sich so schnell – worauf wir uns heute verlassen, wird bereits durch das ersetzt, was jüngere Zielgruppen nutzen, und das ist es, was wir morgen nutzen werden. Die Landkarte verändert sich ständig, und man hinkt immer ein wenig hinterher. Man muss also aufmerksam sein und proaktiv handeln, statt nur zu reagieren.
>
> **– Elliott Champion, CSC Global Product Director, Brand Protection and Anti-Fraud**

Die Bekämpfung von IP-Rechtsverletzungen erfordert eine umfassende, teamübergreifende Denkweise

Unsere Befragten gaben an, dass sie ein relativ hohes Vertrauen in ihre Überwachungs- und Domain-Management-Strategien haben. Die Mehrheit (86 %) gibt an, eng mit anderen Teams, darunter IT und Sicherheit, zusammenzuarbeiten.



der Befragten gaben an, dass sie entweder „äußerst“ oder „ziemlich“ zuversichtlich hinsichtlich der internen Systeme zur Überwachung von IP-Rechtsverletzungen ihres Unternehmens sind.



gaben an, dass ihr Unternehmen über eine Domain-Management-Strategie verfügt, weitere 12 % sind im Begriff, eine solche Strategie zu entwickeln.

Allerdings gaben nur 16 % an, dass ihre Rechtsabteilungen einen „vollständigen” Überblick über die Verwaltung des Domain-Portfolios ihres Unternehmens haben.

„Unternehmen benötigen diesen einheitlichen Ansatz, um Backend-Sicherheitsprobleme zu bewältigen, insbesondere, wenn das Marketing eine bestimmte Kampagne mit einem eigenen Domainnamen plant”, so Mary Jo. „Sie müssen sicherstellen, dass die Rechts-, Sicherheits- und IT-Teams darüber informiert sind, damit sie diese Aktivitäten in die Überwachungsliste aufnehmen können.”

DAS AUFKOMMEN VON DIGITAL GOVERNANCE-TEAMS

Unternehmen mit einem erfolgreichen, proaktiven Ansatz zur Bekämpfung von IP-Rechtsverletzungen haben mit größerer Wahrscheinlichkeit ein offizielles Digital Governance-Team zusammengestellt, das sich aus Vertretern und Vertreterinnen der Rechts- und Marketingabteilung, der IT-Abteilung und der Sicherheitsabteilung zusammensetzt.

„In vielen großen Unternehmen kommuniziert die leitende Person der Rechtsabteilung oft nicht mit derjenigen der IT-Abteilung“, so Elliott. „Sie verstehen die jeweils andere Welt nicht. Als erstes empfehlen wir neuen Kunden und Kundinnen, alle Beteiligten an einen Tisch zu bringen, damit sie dieses Problem aus verschiedenen Perspektiven betrachten können.

„Wenn es eine wichtige Botschaft gibt, die ich vermitteln möchte, dann die, dass die verschiedenen Teams miteinander kommunizieren sollten – und das muss nicht mehr als ein monatliches Treffen sein, aber es ist wichtig, sich gegenseitig auf dem Laufenden zu halten.“

Verstärkte Inanspruchnahme von Outsourcing- Services, einschließlich Domainnamen-Monitoring

Mit der steigenden Zahl von IP-Rechtsverletzungen wird es immer schwieriger, den Aufwand für die Überwachung von Domainnamen und anderen Aktivitäten intern zu bewältigen. Solche Aktivitäten fallen oft in den Zuständigkeitsbereich der Rechtsabteilung, die möglicherweise bereits ausgelastet ist.

Etwas mehr als die Hälfte (56 %) der Befragten gab an, dass sie derzeit zumindest einige Überwachungsaktivitäten auslagern, aber aktiv nach Möglichkeiten zu suchen, weitere Aufgaben auszulagern.

Die Zusammenarbeit mit einem seriösen, etablierten und engagierten Spezialisten verringert nicht nur den Druck auf die Rechtsabteilungen, sondern zeigt auch das Engagement für den Schutz der Kunden und Kundinnen und die Einhaltung regulatorischer Standards. Ebenso wichtig ist, dass solche Partnerschaften einen erheblichen Mehrwert bieten können, indem sie Protokolle und Abwehrmaßnahmen optimieren und gleichzeitig Zugang zu neuen, innovativen Tools und Anwendungen ermöglichen.

„Wenn Sie sich in einem Rechtsstreit wegen Markenrechtsverletzung befinden, wird das Gericht Sie nicht wohlwollend betrachten, wenn Sie den Missbrauch Ihrer Marken in der Vergangenheit nicht überwacht haben“, so Mary Jo. „Genauso können Sie auf die Tatsache verweisen, dass Sie mit einem Partner wie CSC zusammenarbeiten, der die Marktplätze scannt, Verstöße ahndet und es böswilligen Akteuren so schwer wie möglich macht – als Beweis dafür, dass Sie alles in Ihrer Macht Stehende tun, um Ihr geistiges Eigentum zu schützen.“

> CSC ist ein führender Anbieter von Tools, die proaktive Bedrohungsinformationen zu möglichen Domainnamen liefern, die als Ausgangspunkt für einen Angriff dienen könnten. Weil das schnell und proaktiv weltweit möglich ist, können sich Unternehmen besser vor IP-Rechtsverletzungen schützen, die mit gefälschten Domainnamen ihren Anfang nehmen.
>
> „Ein verantwortungsbewusstes Unternehmen, das Bedrohungen durch IP-Rechtsverletzungen ausgesetzt ist, muss über eine mehrschichtige, proaktive Cybersicherheitsstrategie verfügen. Eine Firewall allein reicht nicht aus. Und wer sich noch nicht mit Outsourcing-Strategien für die Überwachung von IP-Rechtsverletzungen und die Domainverwaltung befasst hat, verpasst den Anschluss.“
>
> **– Ian McConnel, CSC Chief Legal Officer**

REGISTRARE FÜR PRIVATPERSONEN IM VERGLEICH ZUREGISTRAREN FÜR UNTERNEHMEN – WAS IST DER UNTERSCHIED?

Um zu beurteilen, wie Domainnamen überwacht und geschützt werden können, ist es unerlässlich, die Unterschiede zwischen Registraren für Privatpersonen und Unternehmen zu verstehen. Ihab hebt fünf wesentliche Unterschiede hervor.

1. **Durchsetzungsfähigkeit:**Registrare für Unternehmen bieten eine globale, effektive und intelligente Durchsetzung (oder Takedowns), während Registrare für Privatpersonen nicht über die erforderlichen Tools und Kompetenzen verfügen.
2. **Geschäftlicher Schwerpunkt:** Registrare für Privatpersonen sind hauptsächlich auf den Verkauf von Domainnamen ausgerichtet und fungieren als Vermittler, während sich Registrare für Unternehmen auf die Verwaltung und den Schutz von Domainnamen sowie die Minderung globaler Risiken konzentrieren.
3. **Hosting-Sicherheit:** Registrare für Privatpersonen können Webserver für das Hosting von Domains zur Verfügung stellen, diese werden jedoch oft unzureichend gewartet und nutzen unter Umständen unsichere, gemeinsam genutzte Infrastrukturen.
4. **Sicherheitsstandards:**Registrare für Unternehmen verfügen über robustere Sicherheitsmaßnahmen zum Schutz der Domain-Portfolios ihrer Kunden und Kundinnen – Sicherheitsmechanismen, mit denen Registrare für Privatpersonen nicht mithalten können.
5. **Überwachungsreichweite:** Registrare für Unternehmen überwachen weltweit E-Commerce- und Auktionsseiten, um den Missbrauch von Domainnamen aufzudecken, während Registrare für Privatpersonen in der Regel erst dann tätig werden, wenn ein Problem festgestellt wurde.

„Betrügerische Akteure greifen Markeninhaber:innen mit drei Haupttaktiken an: Markenmissbrauch, Identitätsdiebstahl und Produktfälschungen“, erklärt Ihab. „Um diesen Bedrohungen effektiv zu begegnen, benötigen Sie einen Registrar für Unternehmen mit einer Durchsetzungsabteilung – alles andere reicht nicht aus.“

Es ist Zeit zu handeln, bevor es zu spät ist

Die Anzahl und Vielfalt der Angriffe auf das geistige Eigentum von Unternehmen nimmt weiter zu. Die Einstiegshürden für betrügerische Akteure sind aufgrund von Technologien wie KI und CaaS-Toolkits deutlich geringer geworden. Unsere Studie zeigt, dass Juristen im Allgemeinen davon überzeugt sind, die angemessenen Richtlinien und kooperativen Arbeitspraktiken zur Bekämpfung dieser Risiken implementiert zu haben. Ohne eine mehrschichtige, proaktive Cybersicherheitsstrategie wird es jedoch immer schwieriger werden, mit den eskalierenden Bedrohungen Schritt zu halten.

Die Zusammenarbeit mit einem vertrauenswürdigen Partner bei der Einrichtung einer proaktiven Sicherheitsstrategie schafft einen klaren, effektiven Weg zum Schutz des geistigen Eigentums und gibt Kunden und Kundinnen sowie Stakeholdern die Gewissheit, dass angemessene Sicherheitsvorkehrungen getroffen wurden.

„Proaktives Handeln zeigt, dass Sie Ihr Eigentum und Ihr geistiges Eigentum schätzen“, so Mary Jo. „Auf lange Sicht zahlt es sich aus – nicht nur durch Erkennung und Überwachung, sondern auch durch die Sicherstellung, dass Sie über die richtigen rechtlichen Durchsetzungs- und Deaktivierungsmechanismen verfügen.“

Ein proaktiver Ansatz, insbesondere in Zusammenarbeit mit einem erfahrenen Drittanbieter, ist auch zeit- und ressourceneffizienter.

„Die Folge einer nicht proaktiven Vorgehensweise ist, dass Sie mehr Abhilfemaßnahmen ergreifen müssen“, fasst Elliott zusammen. „Was in einer Besprechung mit CSC fünf Minuten in Anspruch nehmen würde, könnte ohne die Hilfe eines Dienstleisters für Unternehmen fünf Monate dauern und zusätzliche Kosten verursachen, um eine Domain wiederherzustellen.“

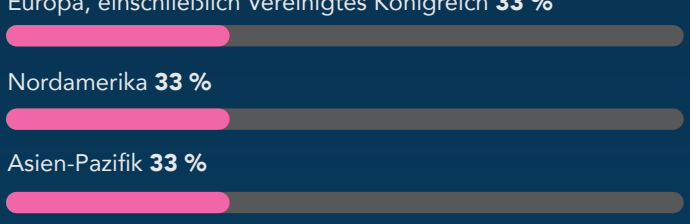
Abschließend unterstreicht Ihab den Zusammenhang zwischen IP-Schutz und finanziellen Risiken sowie Reputationsrisiken.

„IP ist untrennbar mit Reputation verbunden, denn Ihre Reputation hängt heutzutage von Ihrer Online-Präsenz ab. Angesichts der massiven Zunahme neuer Bedrohungsvektoren muss diese heute anders geschützt werden als in der Vergangenheit.“

Übersicht über unsere Befragten

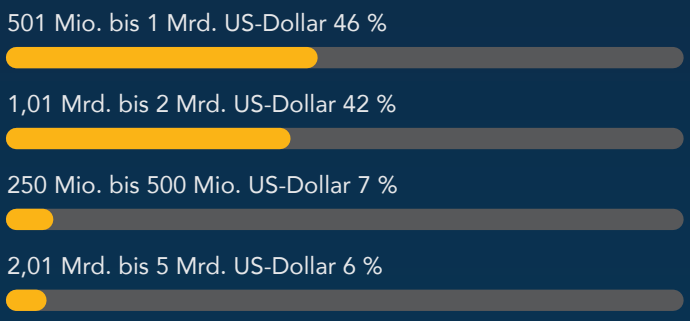
Anzahl der Unternehmen nach vertikalen Sektoren

Hauptsitz der Unternehmen nach Region



Berufsbezeichnung der Befragten

Jahresumsatz der Unternehmen



Sprechen Sie mit uns

1 800 927 9800 | cscdbs.com

Über CSC

CSC ist der vertrauenswürdige Anbieter von Sicherheit und Threat Intelligence der Wahl für Unternehmen im Forbes Global 2000 und für die 100 Best Global Brands (Interbrand®) mit Schwerpunkten in den Bereichen Domainsicherheit und -management sowie digitalem Markenschutz und Betrugssicherung. Angesichts der erheblichen Investitionen, die globale Unternehmen in ihre Sicherheitsposition tätigen, kann unsere Plattform DomainSecSM ihnen helfen, bestehende Versäumnisse in puncto Cybersicherheit zu verstehen und ihre digitalen Online-Vermögenswerte und -Marken zu schützen. Durch den Einsatz der firmeneigenen Technologie von CSC können Unternehmen ihren Sicherheitsstatus verbessern, um sich vor Cyberbedrohungen zu schützen, die auf ihre Online-Vermögenswerte und den Ruf ihrer Marke abzielen. So können sie verheerende Umsatzeinbußen vermeiden. CSC bietet darüber hinaus Online-Markenschutz – eine Kombination aus Online-Markenüberwachung und Durchsetzungsmaßnahmen – einschließlich einer mehrdimensionalen Übersicht über verschiedene Bedrohungen außerhalb der Firewall, die bestimmte Domains ins Visier nehmen. Unsere Lösungen werden ergänzt durch Betrugspräventionsdienste, die Phishing bereits in der Frühphase des Angriffs bekämpfen. Der Hauptsitz von CSC befindet sich seit 1899 in Wilmington, Delaware, USA. Das Unternehmen betreibt Niederlassungen in den Vereinigten Staaten, Kanada, Europa und im asiatisch-pazifischen Raum. CSC ist ein globales Unternehmen und kann überall dort tätig sein, wo unsere Kunden sind. Dies erreichen wir, indem wir in jedem Geschäftsbereich, den wir bedienen, Experten beschäftigen. Besuchen Sie cscdbs.com.

DBS10222025