

# Ein Blick in die Welt der Videopiraten

## ... und wie sie sich aufhalten lassen

Downloading...

Critical Data



# Inhaltsverzeichnis

Die Geschichte der Videopiraterie .....	1
Müssen wir das Problem der Videopiraterie überhaupt lösen? .....	2
Wie funktioniert das Geschäft mit Piraterie? .....	7
Können wir Piraterie aufhalten? .....	13
360-Grad-Ansatz .....	15
Fazit .....	20

## Ein Blick in die Welt der Videopiraten

## Die Geschichte der Videopiraterie

Videopiraterie ist kein neues Problem: Schon seit Beginn der professionellen Filmproduktion versuchen Kriminelle, mit der illegalen Weitergabe von Privateigentum – hier in Form von Urheberrechtsverletzungen – schnell an Geld zu kommen. So entstand während der Stummfilmzeit das sogenannte „Bicycling“. Hierbei wurden legal gemietete Filme entgegen den Vertragsbedingungen mehrmals oder in mehreren Kinos vorgeführt. Dieser Trend wurde so beliebt, dass Hollywood Personen damit beauftragte, diese Kinobesitzer auf frischer Tat zu ertappen. Daraufhin folgten die „Dupers“, also die Duplizierer. Sie erstellten illegale Kopien der Filme, indem sie mit Positivdrucken neue Negative herstellten. Mit fortschreitender Technologie traten sogenannte „Cam-Rips“ auf den Plan, also illegal von der Leinwand abgefilmte Kopien. Sie waren besonders in den 60er Jahren unter Filmdieben sehr beliebt und wurden von der Branche als „Videos mit unbestimmtem Ursprung“ bezeichnet. Doch erst in den 80er Jahren – mit Aufkommen des VHS – wurde die Filmpiraterie zu einem wirklich lukrativen Geschäft mit der Möglichkeit zur Skalierung. Wer in dieser Zeit aufgewachsen ist, weiß wahrscheinlich noch, wie einfach man damals an ganze Kisten mit CDs der neuesten Kinofilme kam – meist jedoch in äußerst fragwürdiger Qualität.

In den 80er und 90er Jahren, in denen Inhalte ohne große technische Erfahrung über physische Methoden gestohlen werden konnten, wie z. B. über DVDs, wurde das Problem der Piraterie deutlich komplizierter. Zum einen agierten Filmdiebe dank der immer besseren Internetverbindungen zunehmend online. Die sogenannte „Warez“-Szene (Internetslang für „Waren“), die mit der illegalen Verbreitung von Videospiele begann, aber sich mit der Zeit auf alle Formen der Piraterie erweiterte, entwickelte eine der ersten echten Internet-Subkulturen. Zwar sind die Warez-Gruppen nicht allein für das Wachstum der Videopiraterie verantwortlich, jedoch spielten sie – und spielen sie immer noch – eine entscheidende Rolle bei der Beschaffung und Verbreitung von Inhalten.

Zum anderen erlebten wir mit dem Wachstum des Pay-TV in den 80ern und 90ern neue Arten der Piraterie, wie z. B. den illegalen Zugriff auf verschlüsselte Übertragungen. Das förderte zwar die schnelle Entwicklung bedingungsbasierter Zugriffstechnologien, doch durch den hohen potenziellen Gewinn und die gestiegene technische Komplexität wurden auch die Kriminellen mit der Zeit immer raffinierter, organisierter und ökonomischer.

In dieser Zeit kamen darüber hinaus neue Anbieter auf, die die unautorisierte Weitergabe von Dateien über das Internet vereinfachten (das sogenannte „Sharing“). Napster war der Ursprung dieses Konzepts. Zwar musste Napster 2001 aus rechtlichen Gründen eingestellt werden, jedoch traten im Anschluss immer mehr P2P-Filesharing-Sites auf den Plan. P2P steht für Peer-to-Peer, was frei übersetzt so viel wie „Nutzer-zu-Nutzer“ bedeutet. Mit diesen Sites ließen sich auf äußerst einfache Weise Tausende gestohlene Videokopien sofort an Millionen von Nutzern verbreiten. Die neue Generation der Sharing-Plattformen war technisch raffinierter und Protokolle wie Morpheus, Gnutella, LimeWire, eMule und BitTorrent florierten. Die Plattformen und Protokolle speicherten die urheberrechtlich geschützten Inhalte in der Regel nicht auf einem zentralen Server, sondern ermöglichten die direkte Weitergabe unter Nutzern (Peers), um Haftung und Anfälligkeit zu vermeiden.

### Ein Blick in die Welt der Videopiraten



*Die Warez-Szene entwickelte damals eine der ersten echten Internet-Subkulturen.*

Und je besser die Zuschauererlebnisse offizieller digitaler Videotechnologien über das Internet wurden, desto weiter entwickelten auch die Filmdiebe ihre Angebote. Heute nutzen Videopiraten verschiedenste Angriffsvektoren, um Inhalte abzurufen und zu verbreiten. Das erneute Streamen linearer Kanäle (Restreaming) kann Nutzern Erlebnisse bieten, die vom echten Fernsehen nicht zu unterscheiden sind. Cyberlocker, wie z. B. Megaupload (heute: Mega), nutzen Cloud-Speicher, die an Orten gehostet werden, an denen Urheberrechte nicht durchgesetzt werden. Die Mittel zur Verbreitung sind vielseitig und leistungsstark, darunter Streaminggeräte oder -websites. Piraterieunternehmen bieten Kunden oft einfache Nutzererlebnisse, Kundenservice und eine Reihe flexibler Geschäftsmodelle. Eine der Personen, die wir für dieses Whitepaper befragt haben, sagte sogar, dass die legale Videostreamingbranche einiges von den Piraten lernen könnte.

Mit diesem Aspekt im Hinterkopf untersuchen wir in diesem Whitepaper die Herausforderungen rund um den Diebstahl geistigen Eigentums und stellen uns die Frage, ob sich Piraterie überhaupt aufhalten lässt.

## Müssen wir das Problem der Videopiraterie überhaupt lösen?

Bevor wir untersuchen, ob Videopiraterie aufgehoben werden *kann*, müssen wir zunächst herausfinden, ob sie überhaupt aufgehoben werden *muss* – so unerwartet das für ein Whitepaper zum Thema klingen mag. Film- und Fernsehbranchen läuten ein neues technisches und kommerzielles Zeitalter ein. Sendeanstalten und Filmverleihe müssen zahlreiche Anforderungen in puncto Betriebs- und Investitionskosten erfüllen (die oft in Konflikt zueinander stehen), um die Produktion, neue technische Formate und oftmals auch neue Geschäftsmodelle zu unterstützen. Deshalb werden Mittel zur Bekämpfung der Piraterie gemeinsam mit anderen Anforderungen im Unternehmen priorisiert. Angesichts dieser Umstände müssen wir den relativen Wert und den potenziellen Return on Investment genau bestimmen.

Früher hat die Branche im Durchschnitt etwa ein Prozent der Lizenzierungskosten in Anti-Piraterie-Maßnahmen investiert. Mit der Zeit nahm dieser Wert jedoch ab, da der bedingte Zugriff immer zuverlässiger wurde und Pay-TV-Betrug effektiv verhindern konnte. Zwar ist IP-basierte Videopiraterie nichts Neues, doch in einem Whitepaper von Parks Associates zum Thema Videopiraterie heißt es, dass sich die Medienbranche in einer Early-Adopter-Phase befindet. So kommt das Unternehmen zu dem Schluss, dass sich die meisten Bemühungen bisher auf die Diebstahl- oder Weiterverbreitungsprävention konzentrieren. Anbieter sollten jedoch stattdessen eher ein Auge auf Credential Stuffing haben. Müssen wir diesen Punkt angesichts der Verschiebung des Videomarktes hin zu reinen IP-Methoden und angesichts der neuen Verbreitungsmethoden von Filmdieben nun neu bewerten? Um diese Frage zu beantworten, müssen wir zunächst das zugrunde liegende Problem genau verstehen. Wie weit ist Videopiraterie global und in unterschiedlichen Regionen verbreitet und welche Folgen hat sie auf Medienunternehmen?

## Das Ausmaß des Problems

Es gibt zahlreiche herausragende Studien zum Thema der Videopiraterie. Doch auch mit diesen Studien ist das wahre globale, regionale und nationale Ausmaß der Videopiraterie nur schwer zu bestimmen. Grund hierfür sind fehlende einheitliche Methoden, mit denen sich das Problem nachverfolgen lässt. Dementsprechend können die vielen unterschiedlichen Informationen für Verantwortliche, die Prioritäten setzen müssen, ziemlich verwirrend sein.

## Ein Blick in die Welt der Videopiraten

Datensätze, die von kommerziellen Unternehmen bereitgestellt werden, sind zwar oft nützlich, können jedoch den Daten widersprechen, die mit anderen Methoden erhoben wurden. Und nicht kommerzielle Studien sind zwar oft gründlich, beschränken sich jedoch in der Regel aufgrund gesetzlicher Grenzen auf bestimmte Länder oder Ländergruppen. Auch die in den verschiedenen Berichten verwendete Terminologie ist nicht standardisiert, was bei Lesern ebenfalls zu Verwirrungen führen kann. Und zu guter Letzt sind absolute Zahlen nur schwer zu definieren, da viele Nutzer gestohlener Medien auch legale Services nutzen.

Laut einem der Befragten für dieses Whitepaper ist Videopiraterie eine echte Sisyphusarbeit. Jeder kennt die allgemeinen Angriffsvektoren und die Verbreitungsmethoden, doch niemand weiß genau, welche von ihnen vorherrschend sind – insbesondere bei der Art des eigentlichen Diebstahls.

Einige jüngere Studien verwenden jedoch eine wiederholbare Methodik, um den Umfang der Piraterie zu bestimmen. So führte beispielsweise das Amt der Europäischen Union für geistiges Eigentum (EUIPO) eine Studie über die Folgen der Piraterie in den EU-Mitgliedstaaten durch. Das Amt fand heraus, dass 13,7 Millionen Personen in EU-Ländern auf illegale Piraterieservices verschiedener Arten zugreifen. Die Studie ergab außerdem, dass die Niederlande (8,9 %), Schweden (8,5 %) und Spanien (6,9 %) die höchsten Prozentsätze entsprechender Nutzer aufweisen. Der europäische Durchschnitt liegt bei 3,6 Prozent. Das Vereinigte Königreich (2,4 Millionen), Frankreich (2,3 Millionen) und Spanien (2,2 Millionen) sind führend bei Einwohnern, die regelmäßig illegale Services nutzen. Und nun machen Sie sich doch einmal die Diskrepanzen bei der Forschung zum Piraterieumfang bewusst: Eine kürzlich erschienene YouGov-Studie kam zu dem Schluss, dass im gesamten Vereinigten Königreich 4,9 Millionen illegale Kodi-Boxen im Einsatz waren. In Europa hat die Piraterie im Gegensatz zu anderen Regionen abgenommen. Die genauen Zahlen sind zwar nicht ganz klar, fest steht jedoch, dass diese Entwicklung das Ergebnis einer Kombination verschiedener Punkte ist: zum einen die Festnahme und strafrechtliche Verfolgung von Videopiraten, zum anderen die erneuten Bemühungen einiger Regierungen, ihre Bürger über die Schäden der Piraterie zu informieren.

**13,7 Millionen**  
*geschätzte Nutzer  
von gestohlenen  
Videoinhalten in  
der EU*

In Nordamerika ist das Bild nicht so deutlich. Sandvine hat die Nutzung mehrerer fester Tier-1-Netzwerke analysiert und kam zu der Schätzung, dass 6,5 Prozent der Haushalte regelmäßig mit Piraterieseiten kommunizieren. Park Associates hingegen berichtet, dass 2019 über 14,1 Millionen US-Haushalte auf gestohlene Videoinhalte zugegriffen haben – was in etwa 16 Prozent des gesamten Pay-TV-Marktes ausmacht. Zwar lassen sich diese Zahlen mit denen der EU vergleichen, jedoch werden durch Unterschiede in der Methodik möglicherweise die Herausforderungen der Region unterschätzt.

Im Asien-Pazifik-Raum sieht das Ganze deutlich komplexer aus. In dieser vielfältigen Region ohne einheitliche Aufsichtsbehörde werden die meisten Studien nur in spezifischen Ländern und in der Regel von kommerziellen Unternehmen oder Brancheneinrichtungen durchgeführt. Die verfügbaren Forschungsdaten zeigen jedoch, dass die Region einige der intensivsten Nutzer gestohlener Inhalte beheimatet.

Eine Studie der Universität Amsterdam aus dem Jahr 2017 hat Nutzergewohnheiten rund um Videopiraterie in Hongkong, Indonesien, Japan und Thailand untersucht. Die Studie ergab, dass die Bevölkerung von Indonesien und Thailand mit 65 bzw. 54 Prozent der Internetnutzer eine hohe Dichte hinsichtlich gestohlener Inhalte aufweist. In Hongkong waren es 27 Prozent der Internetnutzer und in Japan nur 12 Prozent (11 % der Gesamtbevölkerung).

Eine unabhängige Verbraucherstudie, die 2019 von der Asia Video Industry Association in Auftrag gegeben wurde, bekräftigte diese Ergebnisse und ergab, dass in Hongkong 24 Prozent der Verbraucher Streamingsservices nutzen, um auf gestohlene Videoinhalte zuzugreifen. Dieser Wert steigt bei den Philippinen auf 28, bei Taiwan auf 34 und bei Thailand auf 45 Prozent.

Anhand dieser Zahlen können wir erkennen, dass die Videopiraterie – insbesondere die TV-Piraterie – weiterhin ein ernsthaftes globales Problem darstellt. Doch wir müssen auch die Folgen der Piraterie ermitteln, um herauszufinden, ob wir weitere Zeit und Ressourcen in die Lösung dieses Problems investieren sollten.

## Welche Folgen hat Piraterie?

Ein Bereich, der bereits umfassend erforscht und beschrieben wurde, sind die Auswirkungen der Videopiraterie auf die langfristige Nachhaltigkeit des Geschäftsmodells Medien. Die meisten Befragten sind sich über die strategischen Herausforderungen einig, jedoch gibt es bei den absoluten Zahlen deutliche Abweichungen. Warum dieser Faktor so wichtig ist, wird deutlich, wenn man den relativen Wert von Investitionen in Anti-Piraterie-Initiativen gegenüber Investitionen in andere Geschäftsanforderungen abwägt. Es gibt viele Faktoren, die bei der Untersuchung der Pirateriefolgen berücksichtigt werden können, darunter die Verbreitung von Malware und anderen Cyberbedrohungen. Für dieses Whitepaper haben wir uns jedoch auf drei wichtige Bereiche konzentriert, auf die sich Piraterie auswirkt: Finanzen, Beschäftigung und Lizenzierung.

## Finanzielle Auswirkungen der Piraterie

Die negativen finanziellen Folgen von Videopiraterie sind den meisten Befragten bekannt. Studien schätzen die Verluste der globalen Branche auf bis zu 52 Milliarden US-Dollar bis 2022 (Digital TV Research, 2017). Und die BIP-Verlustschätzungen fallen aufgrund der niedrigeren Steuern sogar noch höher aus. Allein in den USA werden die BIP-Verluste durch Piraterie auf 47 bis 115 Milliarden USD geschätzt (Blackburn u. a., 2019).

Trotz dieser horrenden Zahlen sehen viele Verleiher die Prävention von Piraterie weiterhin als reinen Kostenpunkt für ihr Unternehmen anstatt als positiven Umsatztreiber. Die Gründe hierfür sind komplex, aber nicht von der Hand zu weisen. Zum einen lässt sich nur schwer nachweisen, dass die Piraterieprävention zusätzliche Umsätze mit sich bringen würde. So zeigt die Forschung, dass Piraterie sogar manchmal zu zusätzlichen Abonnements führen kann, da sie im Grunde kostenlos Werbung für legale Services macht (Sanchez, 2012). Durch dieses „kostenlose Probieren“ lernen Zuschauer auch neue Schauspieler und Genres kennen, was sich über kostenpflichtige Geschäftsmodelle vielleicht gar nicht erreichen lässt (das ist natürlich vom Genre und der Verfügbarkeit legaler Alternativen abhängig). Studien zeigen, dass Nutzer, die Inhalte aus illegalen Quellen beziehen, auch die größten Kunden der legalen Videobranche sind. Hierbei handelt es sich um Verbraucher, die an Filmen oder Serien interessiert sind und deshalb über jeden verfügbaren Kanal mehr konsumieren. Deshalb sind die legale und die illegale Nutzung von Personen nicht vergleichbar und Anbieter kommen zu dem Schluss, dass sämtliche finanziellen Verluste kausal damit zusammenhängen.

Auch die Weitergabe der Anmeldeinformationen für Medienservices gilt zwar als Piraterie, wird jedoch von den meisten SVOD-Services (abonnementsbasiertes Video-on-Demand) aus Marketingzwecken geduldet. In den Worten eines CTO: „Wir wissen, dass es passiert, aber wir wissen auch, dass die Nutzer irgendwem als Kunden bei uns landen.“

Die zweite Herausforderung bei der Untersuchung finanzieller Verluste besteht darin, dass Forscher oftmals einen „Multiplikatoreffekt“ anwenden, was zu einer Überschätzung der finanziellen Auswirkungen auf die Branche führen kann. Hierzu ein Beispiel: Die Motion Picture Association of America (MPAA, jetzt MPA) gab zu, dass das Problem durch die angegebenen finanziellen Verluste infolge von Piraterie in einem ihrer Berichte stark übertrieben dargestellt wurde (Greenburg, 2015; Sanchez, 2012).

Die finanziellen Folgen der Videopiraterie weichen daher regional, national und auch je nach Unternehmen stark ab. Eine Studie der Universität Amsterdam 2017 befasste sich mit der Komplexität bei der Ermittlung der globalen finanziellen Folgen von Piraterie. Die Studie ergab, dass individuelle nationale Haltungen weiterhin nennenswerte Auswirkungen auf die Piraterieverbreitung haben. Beispiele hierfür finden sich sowohl in Industrie- als auch in Entwicklungsländern, in denen ein Urheberrecht vorhanden ist. Diese Verwirrung hat eindeutig Zweifel in den Köpfen von Sender- und Studioleitungen gesät – ganz besonders bei der Budgetpriorisierung.

Abgesehen davon werden die erheblichen Folgen – also wenn ein Zuschauer nach Nutzung illegaler Quellen nicht zur legalen Variante wechselt oder legale Services sogar verdrängt werden – als ernsthafte Herausforderung für die Branche anerkannt. Eine von der US-Handelskammer in Auftrag gegebene und 2019 veröffentlichte Studie ergab, dass die gesamten globalen Umsatzverluste durch digitale Videopiraterie (also durch Verdrängung legaler Services und andere Faktoren) 2017 zwischen 40 und 97,1 Milliarden US-Dollar für die Filmbranche und zwischen 39,3 und 95,4 Milliarden USD für die TV-Branche lagen. In den USA wurden 2,5 Milliarden USD (Film) bzw. 3,6 Milliarden USD (TV) berechnet. Das zeigt, dass Videopiraterie eher ein globales Problem ist.

**79,3-192,5  
Mrd. USD**  
*geschätzte Kosten der  
globalen Piraterie in  
der Film- und  
Fernsehbranche*

Verglichen mit den finanziellen Verlusten durch Verdrängung lassen sich die finanziellen Gewinne der Videopiraten klarer bestimmen. Es wird geschätzt, dass das Geschäft mit gestohlenen Videoinhalten innerhalb der Europäischen Union einen Jahresumsatz von etwa 941,7 Millionen Euro verzeichnet – über kostenpflichtige Abonnements und Werbung. Das Vereinigte Königreich, Frankreich, Deutschland, die Niederlande und Spanien generieren nahezu 76 Prozent dieser Umsätze (EUIPO, 2019). Sandvine geht davon aus, dass das Piraterieökosystem in den USA ähnliche Zahlen erreicht: mit Umsätzen von über einer Milliarde. Es wurden bisher keine Studien in den Regionen Asien-Pazifik und Südamerika durchgeführt, die uns vergleichbare Zahlen bieten würden.

### **Auswirkungen der Videopiraterie auf die Beschäftigung**

Die meisten Berichte zu den Folgen der Piraterie konzentrieren sich auf den Umsatzverlust. Die Film- und Fernsehbranche beschäftigt jedoch auch Millionen von Angestellten – von Set-Designern und Make-up-Artists über Musiker bis hin zu Regisseuren und Produzenten – und Piraterie schadet ihnen allen. Bis vor Kurzem basierten Studien zur Verbindung zwischen Videopiraterie und Stellenabbau größtenteils auf öffentlichen Ankündigungen von Services, die ihren Betrieb verkleinern oder einstellen mussten. So gab beispielsweise beIN bekannt, dass als direkte Folge von Piraterie 300 Stellen gestrichen werden, und RTL International verkündete die Einstellung seiner internationalen Pay-TV-Kanäle. Ein weiteres interessantes Beispiel ist die Absetzung der Psycho-Thriller-Serie *Hannibal* aufgrund „schlechter Einschaltquoten“. Die Serie wurde jedoch im Jahr 2013 als die Nummer fünf unter den am häufigsten illegal heruntergeladenen Serien eingestuft. „Enttäuschte Fans der Serie können die Schuld nur bei sich selbst und ihren Mitzuschauern suchen“, erklärt Produzentin Martha De Laurentiis, laut der Piraterie eine wichtige Rolle für die Absetzung spielte.

### **Ein Blick in die Welt der Videopiraten**

Dank neuer, umfangreicherer Studien zu dem Thema können wir die breiten Folgen heute besser erkennen. In ihrem Bericht zu den Folgen der Videopiraterie auf die US-Wirtschaft kamen Blackburn, Eisenach und Harrison zu dem Schluss, dass 2017 in den USA zwischen 230.000 und 560.000 Stellen aufgrund von Piraterieaktivitäten verloren gingen. Bei den Stellenverlusten wurden sämtliche Bereiche der Branche berücksichtigt, darunter sowohl direkte als auch indirekte, kreative wie nicht kreative Funktionen.

Zum Stellenabbau außerhalb der USA wurden weniger vergleichbare Studien durchgeführt. Das liegt an der ungleichen Verteilung der Funktionen in den verschiedenen Ländern – die USA hingegen sind ein homogener Markt. Studien der Organisation zum Schutz von audiovisuellen und Multimedia-Inhalten (FAPAV) in Italien ergaben jedoch, dass nahezu 6.000 direkte Stellen durch Piraterie verloren gingen. Auch hier wurden die betroffenen Funktionen, die mit der Medienproduktion und -verbreitung in Verbindung stehen, breiter ausgelegt. Dank der Methodik der FAPAV lassen sich die Zahlen aus Italien auch auf Stellenverluste in den übrigen EU-Mitgliedstaaten übertragen. In Ländern mit starkem Fokus auf Inhaltsproduktion und -export, wie z. B. im Vereinigten Königreich, Spanien und Deutschland, könnten diese Zahlen sogar noch höher ausfallen.

Hierbei ist zu beachten, dass einige Forscher die Folgen der Piraterie auf die Beschäftigung deutlich geringer einschätzen. Verschiedene Experten stellen den Verdrängungsfaktor und die wahren Auswirkungen der Piraterie auf den erzielten Branchenumsatz (und somit auf die Beschäftigung) infrage. Einige Forscher kamen zu dem Schluss, dass die Messung entgangener Chancen eine bessere Kennzahl zur Einordnung von Beschäftigungseinbußen darstellt. Das liegt daran, dass in der Produktion viele freiberufliche Kreativarbeiter zum Einsatz kommen, die bei pirateriebedingt verringerten Programminvestitionen möglicherweise nicht vollständig ausgelastet werden. Darüber hinaus wird auch darauf verwiesen, dass der aktuelle Aufschwung im Produktionssektor, der teilweise durch Investitionen der SVOD-Services verursacht wird, die negativen Folgen der Piraterie auf die Beschäftigung reduziert.

Trotz der laufenden Debatte über das Verdrängungspotenzial der Piraterie ist klar, dass Urheberrechtsverletzungen deutliche Folgen auf die Beschäftigung – oder besser: auf Beschäftigungschancen – haben. Bei einem so umfangreichen Produktdiebstahl würde es wohl jeder Branche schwer fallen, die volle Beschäftigungsquote aufrechtzuerhalten. Die Folgen sind in Ländern oder Unternehmen mit starkem Produktionsfokus oder internationalen Sendern wahrscheinlich stärker spürbar.

### **Auswirkungen der Videopiraterie auf die Lizenzierung**

Wir haben bereits erste Anzeichen dafür erlebt, dass Piraterie die Lizenzierung beeinträchtigt. Und da die Lizenzierung das Herzblut der Kreativbranche darstellt, ist dieses strategische Problem dringender als jedes andere. Einfach ausgedrückt: Warum sollten potenzielle Verleiher erhebliche Summen für Rechte bezahlen, wenn Inhalte einfach und kostenlos auf Piraterieseiten verfügbar sind? Und umgekehrt: Warum sollten Rechteinhaber an einen nicht vertrauenswürdigen Verleiher vertreiben, wenn sie hierdurch womöglich ihren internationalen Verkäufen schaden?

Das Sportgenre ist hierbei besonders anfällig, was jüngste Schlagzeilen beweisen. Laut Yousef Al-Obaidly, Chief Executive von beIN, einem der größten weltweiten Käufer von Sportrechten, ist „die Blase der Sportrechte durch globale Piraterie kurz davor, zu platzen“. Er betont, dass der Wert der Rechte für sein Unternehmen auf dem Maß an Exklusivität basiert. Wenn Inhalte aufgrund von Piraterie nicht mehr exklusiv sind, verringert sich ihr Wert deutlich.

In einem anderen Artikel beschreibt Jason Blum, Oscar-Nomierter und Emmy-Award-Gewinner, die direkten Folgen der Piraterie auf die Bereitstellung der Mittel für innovative und gewagtere Filme, die die Grenzen des Storytellings erweitern. Er ist der Meinung, dass irgendwann in nicht allzu ferner Zukunft die Zahlen nicht mehr tragbar sein werden und Studios entsprechende Produktionen streichen müssen. „Sie werden nicht ihre Franchises (mit denen sie das meiste Geld verdienen) oder Low-Budget-Horrorfilme reduzieren, sondern Kunstfilme, die riskant und oft nicht sonderlich rentabel sind. Schon bald gibt es keine Filme mehr wie *The Big Short*, die man überhaupt noch stehlen könnte.“

“ **Die Blase der Sportrechte ist durch globale Piraterie kurz davor, zu platzen.**“

- Yousef Al-Obaidly, CEO, beIN

Und so kommen wir zu der Frage zurück: Müssen wir das Piraterieproblem lösen? Auf den ersten Blick sollte für die meisten Verleiher ersichtlich sein, warum die Implementierung von Anti-Piraterie-Strategien sich lohnt - zum Schutz von Kernumsätzen, exklusiven Rechten und Arbeitsstellen. Piraterie ist in allen Regionen verbreitet und wird trotz einiger erfolgreicher Gegenmaßnahmen in der EU in den nächsten Jahren weiter wachsen. Es ist klar, dass Piraterie die Finanzen von Produzenten, Rechteinhabern und Verleihern beeinträchtigt. Was jedoch nicht klar ist, ist das Ausmaß dieser Folgen auf Unternehmensebene. Und das macht es für die Führungsebene äußerst schwierig, Anti-Piraterie-Investitionen zu rechtfertigen.

Ein facettenreiches Thema, das von einer Reihe von Faktoren abhängt: Ist Pay-TV oder Free-TV die vorherrschende Verbrauchsform im jeweiligen Land? Ist das Unternehmen Nettoexporteur der Rechte oder Importeur exklusiver Rechte? Hat das Unternehmen einen Wettbewerbsvorteil innerhalb eines bestimmten Genres, wie z. B. TV-Dramen oder Filme? Anhand der Antworten auf diese Fragen lässt sich eine klare Analyse der finanziellen Risiken erstellen, mit der sich wiederum die geeignete Strategie erarbeiten lässt.

Viele Medienunternehmen stehen unabhängig von ihrem Geschäftsmodell vor denselben strategischen Herausforderungen durch Piraterie, also den Folgen für Beschäftigungschancen und Lizenzierung. Beide sind essenziell für die Gesundheit und langfristige Nachhaltigkeit der Branche, insbesondere angesichts schwindender Finanzierung für Produktionen. Daher können wir davon ausgehen, dass Inhaber von Premiumrechten, Brancheneinrichtungen und sogar Behörden in Zukunft immer stärker darauf bestehen werden, dass Unternehmen im gesamten Ökosystem umfassende Strategien implementieren, um das Problem anzugehen. Diese Strategien untersuchen wir im letzten Abschnitt dieses Whitepapers.

## Wie funktioniert das Geschäft mit Piraterie?

Wie in jedem Kampf ist es auch hier wichtig, seinen Gegner zu kennen: seine Motivation, seine Taktik, seine Stärken und Schwächen. Im Gegensatz zu vielen anderen Aspekten der Videopiraterie gibt es hierzu nur wenige zuverlässige Studien - die Gründe dafür liegen wahrscheinlich auf der Hand.

## Wer sind die Videopiraten?

Studien beschreiben Videopiraten oft als eine ruchlose homogene Gruppe mit einem gemeinsamen Ziel: Geld zu verdienen. Eine schnelle Internetsuche ergibt zahlreiche Artikel, in denen Razzien der Polizei bei einer „Gang von Piraten“ beschrieben werden, die mit ihrer Website Gewinne in Millionenhöhe erzielt haben.

Diese Beschreibungen vermitteln das Bild, dass es sich bei Piraten um organisierte, opportunistische Kriminelle handelt, die ein komplexes, raffiniertes Geschäft betreiben. Und in manchen Fällen ist das definitiv der Fall. Doch wie so viele Aspekte des Internets ist auch die digitale Piraterie inhärent global und anonym. Es lässt sich nur schwer nachverfolgen, wo genau ein gestohlener Film oder eine Serie ihren Ursprung haben oder wer die Inhalte überhaupt gestohlen hat. Wir wissen jedoch, dass es ein komplexes Ökosystem von Gruppen und Untergruppen gibt, die jeweils eigene Beweggründe, individuelle technische Erfahrung und gruppenübergreifende Abhängigkeiten aufweisen.

## Die Releasegruppen

Verschiedene Studien beschreiben Videopiraten als uneigennütige Personen – ganz im Sinne der ursprünglichen Warez-Szene. Mitglieder sehen sich oft als romantisierte Revolutionäre im Kampf gegen Großkonzerne. Und diejenigen, die erwischt und bestraft werden, werden als Helden gefeiert. So sagte der Mitgründer von Pirate Bay, Fredrik Neij, nach Ende seiner 10-monatigen Gefängnisstrafe: „Das Ganze war die Zeit im Gefängnis auf jeden Fall wert, wenn man bedenkt, wie viele Leute dadurch auf die Site gekommen sind.“

In dieser Gruppe verbindet die Piraten ein gewisses Gemeinschaftsgefühl, wenn auch mit einem etwas seltsamen Verständnis von Nächstenliebe. Rein finanzielle Beweggründe sind hier aber nicht unbedingt zu finden. Die Mitgliedschaft bei den Sites, auf die Inhalte hochgeladen werden, müssen sich Nutzer erst verdienen, indem sie beweisen, dass sie würdig sind und dass man ihnen vertrauen kann. Verschiedene Gruppen und Personen sind auf bestimmte Genres spezialisiert und versuchen, möglichst als Erste an brandneues Material zu kommen, um dafür mit Anerkennung belohnt zu werden. Inhalte in schlechter Qualität oder mit Viren werden sofort entfernt und der Uploader ist forthin in der Community verurteilt. In seinem Artikel in der *Vanity Fair* zum Wachstum von Torrents charakterisierte Steve Daly die Mitglieder der Releasegruppe mit den klassischen Stereotypen der Computer-Geeks: sozial schüchterne und von Natur aus obsessive Personen, die durch das Stehlen der Inhalte eine Art von Zugehörigkeitsgefühl erlangen. FACT beschrieb sie hingegen ganz anders: „Es handelt sich hierbei um eine komplexe, raffinierte und gut organisierte hackerähnliche Gruppe, die sich vermeintlich auch an anderen Arten von Cyberverbrechen beteiligt, wie z. B. der Verbreitung von Ransomware oder dem Hacken von Bankkonten zum Verkauf im Dark Web.“ Unabhängig von ihren Beweggründen weisen die Gruppen – wie die Warez-Szene – klare hierarchische Strukturen mit vielen festgeschriebenen Regeln und starken vertrauensbasierten Verbindungen auf.

## Die Sitebetreiber

Die öffentlich zugänglichen Seiten, wie z. B. Cyberlocker oder Streamingseiten, werden von einer anderen Gruppe gemanagt: den Sitebetreibern. Es ist nicht bekannt, ob es sich bei den Releasegruppen und Sitebetreibern um dieselben Gruppen handelt, doch viele Studien kommen zu dem Schluss, dass viele Überschneidungen und deutliche Abhängigkeiten zwischen den beiden bestehen. In jedem Fall verdienen die Sitebetreiber Geld an dem Prozess. Sitebetreiber nutzen oftmals mehrere sogenannte „Mirrorseiten“, die sich gegenseitig duplizieren. Wenn Behörden eine dieser Mirrorseiten offline nehmen, bleibt die Site dennoch verfügbar und erwirtschaftet weiter Gewinne. Wie bei allen professionellen Einzelhandelsbetrieben gibt es auch unter den Websites Großhändler, wie z. B. Streamango und Openload, die gemeinsam über 50 der führenden illegalen Videostreaming- und Videolink-Sites versorgen. Die bekannteste Marke ist jedoch beoutQ, das trotz Einstellung seiner illegalen Feeds über Arabsat weiterhin Inhalte über das Internet verbreitet und laut Expertenaussagen Piraterie im industriellen Ausmaß betreibt. Während die Releasegruppen nicht zwingend finanziell motiviert sind, ist bei Sitebetreibern ein klares Gewinnziel festzustellen. In manchen Fällen umfasst das nur die grundlegenden finanziellen Bedürfnisse zum Betreiben der Site (wie bei den Gründern des oben erwähnten Pirate Bay). In anderen Fällen sind die potenziellen Gewinne jedoch einfach zu verlockend, weshalb Sitebetreiber immer fortschrittlichere Geschäftsmodelle entwickelt haben.

## Ein Blick in die Welt der Videopiraten

## Die Großhändler für Streaminggeräte

Ein weiteres wichtiges Profil der Videopiraterie sind Großhändler für Streaminggeräte. Das Wachstum entsprechender Geräte, insbesondere solcher mit Kodi, bietet eine relativ stabile und vorhersagbare Einnahmequelle für opportunistische Kriminelle, die damit sechsstellige Beträge pro Jahr verdienen können. Großhändler importieren die Boxen oftmals über ganz legale Kanäle und ändern sie dann zu Hause mit illegaler Software. Andere arbeiten mit raffinierten kriminellen Netzwerken zusammen, um Boxen zu importieren und sie online zu verkaufen. Manchmal vertreiben sie so Hunderttausende Boxen, bevor sie erwischt werden. Durch die Verfügbarkeit illegaler Add-ons für Kodi-Software können organisierte Banden ein breiteres Publikum erreichen. Zwar ist Kodi selbst legal, doch die Add-ons sind es nicht. Sie verfügen nicht über Kindersicherungen oder Sicherheitsstandards und setzen Nutzer so zahlreichen Risiken durch nicht jugendfreie und unangemessene Inhalte aus.

## Der Amateurpirat

In jüngster Zeit trat durch Verbesserungen des Livestreamings über Social-Media-Plattformen ein neues Profil auf den Plan: der Amateurpirat. Im Gegensatz zu den Sitebetreibern, den Großhändlern illegaler Streaminggeräte und den Releasegruppen – die von Profit oder organisierter Nächstenliebe angetrieben werden – sind sich die Personen in dieser Gruppe der Tatsache, dass Piraterie illegal ist, weniger bewusst oder es ist ihnen egal. Sie reagieren auf die Preise bestimmter Inhaltsgenres, auf Abonnementmüdigkeit oder auf die Verbreitung von Social Media. Hierzu ein Beispiel: Der Boxkampf zwischen Mayweather und McGregor verzeichnete einen Rekord von 132 Millionen illegalen Aufrufen über mehr als 6.977 illegale Streams. Viele der Streamnutzer waren einfach Verbraucher, die ihre Smartphones vor den Fernseher hielten und den Inhalt über Social-Media-Plattformen verbreiteten.

Es ist wichtig, die Unterschiede zwischen den Piratengruppen zu kennen. Wie bei jeder organisierten kriminellen Aktivität suchen sich Banden mit finanziellen Interessen einfache Ziele aus, um den Gewinn zu maximieren. Stellt man ihnen Hindernisse in den Weg – so simpel sie auch sein mögen –, dann kann hierdurch ein Teil der Aktivitäten abgewehrt werden. Idealistisch motivierte Piraten haben hingegen ganz andere Beweggründe, was es deutlich schwieriger macht, ihre Aktivität zu verhindern.

In fast allen Fällen ist jedoch ein Ökosystem organisierter Teilnehmer vorhanden, das aus primären Content-Dieben (Anbietern illegal bezogener Inhalte), einer Reihe passiver und aktiver Zwischenhändler, Unterstützern, die beispielsweise Kunden bei der Implementierung von Middleware unterstützen, und letztlich den Zuschauern besteht, die das gestohlene Material abrufen. Die letzte Gruppe behandeln wir später im Abschnitt „Wer nutzt gestohlene Inhalte?“.

## Wie beschaffen Piraten Inhalte?

Aufgrund der Verbreitung digitaler Workflows stehen Piraten heute zahlreiche Methoden zur Verfügung, um Inhalte zu stehlen. Aus offensichtlichen Gründen gibt es jedoch äußerst wenige zuverlässige Analysen dazu, welche Methoden am beliebtesten sind und am häufigsten zum Einsatz kommen. Die wenigen verfügbaren Informationen deuten aber auf eine Reihe von Schwachstellen in der gesamten Wertschöpfungskette hin, die ausgenutzt werden können. Um das Ganze zu veranschaulichen, können wir diese Angriffsvektoren nach Anwendungsfall gruppieren.

## Ein Blick in die Welt der Videopiraten



*Schon einfache Hindernisse können einige Aktivitäten abwehren, doch idealistisch motivierte Piraten haben ganz eigene Beweggründe.*

**Simulcast von TV-Sendern und Live-Events:** Eine der am schnellsten wachsenden Formen der Piraterie besteht darin, Inhalte von TV-Sendern oder Live-Events abzugreifen und weiterzuverbreiten. So ergab der Asia Video Industry Report 2019 der Coalition Against Piracy, dass viele Zuschauer, die auf illegale Streaminggeräte umgestiegen waren, auch ihre legalen Aboservices gekündigt hatten und die illegalen Geräte fortan als Haupt-TV-Service nutzten. In Hongkong nutzt beispielsweise ein Viertel der Haushalte entsprechende Geräte und zehn Prozent dieser Haushalte kündigten ihr Abonnement für legale Services. Und durch die Verbreitung von Smartphones - in Verbindung mit Verbesserungen des Livestreamings auf Social-Media-Plattformen - kann heute jeder einfach ein Gerät auf den Fernsehbildschirm richten und Inhalte streamen. Deshalb nutzen Piraten verschiedenste Methoden, um Inhalte von Livesendern abzugreifen, darunter:

- Manipulation von Videowiedergabe-Software oder des Android-Betriebssystems
- Aufzeichnen von Bildschirmen während der Wiedergabe oder Bildschirmfreigabe
- Abfangen verschlüsselter Videosignale mit HDCP-Strippers, die an Set-Top-Boxen angeschlossen werden
- Credential-Stuffing-Angriffe, um auf Anmeldedaten legitimer Nutzer zuzugreifen und diese zu verwenden
- Manipulation von Videos zur Beseitigung von Wasserzeichen, wie z. B. durch Requantisierung
- Transport von Videos außerhalb des jeweiligen Marktes über ein VPN

**On-Demand-Inhalte:** Hierbei handelt es sich ohne Zweifel um die global am weitesten verbreitete Form der Piraterie. Releasegruppen setzen Preise auf neue Video-Assets aus und versuchen, TV-Serien und Filme schon vor deren Release abzugreifen. Interessanterweise werden in diesem Szenario zahlreiche Möglichkeiten der Piraten durch die Struktur der Kreativbranche selbst verursacht. Da so viele Unternehmen und Freiberufler an Produktions- und Postproduktionsprozessen beteiligt sind, bieten sich Piraten zahlreiche Gelegenheiten, Schwachstellen zu finden und auszunutzen. Eine der Personen, die wir für unser Whitepaper befragt haben, veranschaulicht diesen Punkt, indem sie beschrieb, dass Piraten mit dem Internet verbundene Editing-Tools und zugehörige Speicherplattformen einsetzen, um vor der Erstausrahlung auf neue Serien zuzugreifen. Es gibt jedoch noch viele andere Methoden, über die Piraten Video-Assets beschaffen, darunter:

- Angriffe auf Rechenzentren, bei denen Nutzeranmeldedaten, Kryptoschlüssel oder Videoinhalte gestohlen werden
- Diebstahl der Nutzeridentitäten von freiberuflichen und fest angestellten Mitarbeitern, um über verschiedene Systeme auf Videos zuzugreifen
- Aufzeichnungen physischer Assets (heute weniger verbreitet) für Sharing und Verbreitung
- Hacks verschiedener Produktionssysteme, um direkten Zugriff auf Video-Assets zu erhalten
- „Rippen“ (illegales Herunterladen/Umwandeln) von Inhalten aus legalen Quellen, wie z. B. iTunes
- Filmvorführsysteme
- Direkter Diebstahl über Man-in-the-Middle-Angriffe



## Wie verbreiten Piraten Inhalte?

Im Gegensatz zu den Methoden bei der Inhaltsbeschaffung ist dieser Part des Piraterie-Geschäftsmodells gut dokumentiert. Und wie auch beim legalen Streaming nutzen Piraten jeden möglichen Kanal und jede verfügbare technische Innovation:

- Eigens entwickelte IP-Set-Top-Boxen, die auf vorprogrammierte TV-Streams zugreifen
- Software, die auf PCs und Streaminggeräten ausgeführt wird und die Verbreitung gestohlener Inhalte ermöglicht, z. B. Kodi-Add-ons
- Anwendungen, die per Sideloadung auf beliebigen legalen Streaminggeräten installiert werden
- Websites und Social-Media-Services, die nutzergenerierte Inhalte hosten, wie z. B. YouTube
- Websites, die Inhalte über Links an Zuschauer streamen, die einfach per Internetsuche verfügbar sind oder in Social Media gepostet werden
- Klassische Download-, Filehosting-, Cyberlocker- und Torrent-Sites

Zwar ist über die Verbreitungsstrategien der verschiedenen Piratenprofile weniger bekannt, jedoch können wir davon ausgehen, dass Releasegruppen aufgrund der starken Verbreitung eher zu Asset-Sharing-Modellen wie Cyberlockern und Torrent-Sites tendieren. Finanziell motivierte Piraten profitieren hingegen eher von einer Strategie mit illegalen Streaminggeräten und anderen Streamingmodellen, die legale Services nachahmen und mehrere Umsatzmodelle unterstützen. Hierbei ist zu beachten, dass über die Beziehung zwischen den Piratengruppen wenig bekannt ist. Verlassen sich die Sitebesitzer für On-Demand-Assets auf Releasegruppen? Sind sie autonom oder greifen sie auf technisch versiertere Gruppen zurück, um Anti-Piraterie-Kampagnen zu entgehen?

Eine Facette, die die meisten Fälle gemeinsam haben, ist jedoch der Anspruch, Umsatz zu generieren - zumindest, um grundlegende Infrastrukturkosten zu decken. Die meisten Sites verfügen über werbebasierte Umsatzmodelle, doch bestimmte Sites, die Simulcast-Streaming unterstützen, verfolgen mittlerweile einen mehrschichtigen Ansatz, einschließlich Abo- und Hybridmodellen.

TechCrunch berichtete 2008, dass Pirate Bay im Vorjahr unter seinen 2,5 Millionen Abonnenten einen Werbeumsatz von mehr als vier Millionen US-Dollar erwirtschaftet hatte. Und in einem FACT-Bericht aus dem Jahr 2017 heißt es, dass schon kleinere Sites Werbeeinnahmen von über 100.000 USD pro Jahr erzielen können. Zwar sind diese Zahlen kein Vergleich zu denen legaler Unternehmen, jedoch wird davon ausgegangen, dass die Margen der Pirateriesites zwischen 80 und 94 Prozent erreichen (FACT, 2017). Im Vergleich mit den Margen legaler Anbieter, die zwischen 7 und 20 Prozent liegen, lässt sich das große Interesse der Kriminellen leicht nachvollziehen.

Werbung umfasst in der Regel Banneranzeigen oder Pop-up-Fenster für Casinos, Datingseiten, Pornografie oder Downloadservices. Manche Sites enthalten jedoch auch Werbeanzeigen, die über dieselben Technologien bezogen und bereitgestellt werden wie auf legalen Sites. So wissen legitime Marken oft nicht, wo genau ihre Werbung landet, und fragwürdige Sites können ein falsches Gefühl der Legitimität vermitteln. In abobasierten Modellen halten die Piraten ihre Nutzer an, ein Premiumkonto zu erstellen, das gegen eine monatliche Gebühr ein verbessertes Videoerlebnis ohne Werbung bietet. Die Preise für solche Konten fallen je nach Site unterschiedlich aus. Die meisten Seiten bieten verschiedene Pakete mit unterschiedlichen Optionen und Kosten an. Normalerweise bewegen sich die Abopreise jedoch zwischen 5 und 50 Euro.

Doch nicht bei allen Sites läuft es so freundlich ab. Uploader auf Torrent-Sites verdienen wenig bis gar nichts und mit zunehmender Konkurrenz zwischen den Piratensites werden immer mehr Streamingservices auf den Einsatz von Malware, Viren, Adware oder Spamware. Malware wird oftmals so entwickelt, dass sie Piraterie, Identitätsdiebstahl, erzwungenes Kryptomining und verbotene Inhalte, wie z. B. Pornografie, unterstützt. Die Personen, die Malware verbreiten, werden manchmal sehr gut für ihre Bemühungen entlohnt. Eine Studie in den USA legt nahe, dass eine von drei Piratensites ihre Nutzer Malware aussetzt. Hiermit verdienen kriminelle Banden mindestens 70 Millionen US-Dollar pro Jahr, indem sie sich von Hackern dafür bezahlen lassen, die Malware einzubetten (Digital Citizens Alliance, 2017).

In letzter Zeit nutzen Piraten verstärkt neue Möglichkeiten, um Geld zu verdienen, darunter auch Lösegeldforderungen für Inhalte. In diesem Szenario stehlen Hacker Folgen von TV-Serien oder ganze Filme (oder behaupten, sie gestohlen zu haben) und erpressen dann ein Lösegeld von den Produzenten oder Besitzern der Inhalte. Einige dieser Fälle haben es bereits in die Medien geschafft, darunter die 2017er Diebstähle der TV-Serie *Orange Is the New Black* und des Kinofilms *Fluch der Karibik: Salazars Rache*. Grund hierfür war ein Cyberangriff auf HBO, bei dem vermeintlich 1,5 Terabyte an Daten gestohlen wurden. Daraufhin drohten Hacker mit der Veröffentlichung von Folgen und Skripten der Serie *Game of Thrones* (Sulleyman, 2017).

Livestreamings großer Events oder Sportereignisse sind unter Piraten ein besonders beliebtes Ziel. Das liegt zum einen an den hohen Kosten, die Fans aufbringen müssen, um auf legale Feeds zuzugreifen, und zum anderen an der hohen Emotionalität entsprechender Events. In einigen Fällen, wie z. B. bei wichtigen Fußballspielen, gibt es mitunter mehr illegale als legale Streams (Forbes, 2015).

## Wer nutzt gestohlene Inhalte?

Es gibt zahlreiche Studien zu der Frage, warum sich Menschen ohne kriminelle Energie gestohlenen Content ansehen. Darunter finden sich finanzielle Begründungen, bloße Ignoranz und die grundlegende Fähigkeit, ohne irgendwelche Beschränkungen auf Inhalte zuzugreifen. Heute kann jeder mit Internetzugang auf illegale Streamingseiten zugreifen oder mit völlig legalen Geräten alle möglichen Inhalte in hoher Qualität und mit verbraucherfreundlichen Geschäftsmodellen abrufen. Tatsächlich wurde die Verbreitung gestohlener Inhalte über Kodi-Boxen schon als „erfolgreichster Rollout der britischen TV-Geschichte“ beschrieben. Die Beweggründe unterscheiden sich je nach Zuschauer deutlich voneinander. Und auch hier ist es nützlich, erst einmal die verschiedenen Motivationen kennenzulernen, um das Problem wirksam zu bekämpfen.

In einer Studie zur Nutzung gestohlener Inhalte ermittelte VFT verschiedene Nutzerprofile und ihre Beweggründe, die hier zusammengefasst sind:

- a) Die „Content-Anarchisten“ glauben an frei verfügbaren und uneingeschränkten Zugriff auf Onlineinhalte und halten Gebühren jeglicher Art für inakzeptabel. Content-Anarchisten sind der festen Meinung, dass Piraterie nicht illegal ist.
- b) Die „Robin Hoods“ sind weniger extrem in ihren Ansichten und offen für alternative legale Angebote. Diese Gruppe hat sich den Grundsätzen des Content Sharing verschrieben und fördert deshalb die Verbreitung von Dateien.



Bei wichtigen Fußballspielen gibt es mitunter mehr illegale als legale Streams.

- c) Die „Utilitarier“ rechtfertigen ihre Aktionen damit, dass der Inhalt nur einen geringen Wert habe. Angehörige dieser Gruppe kaufen nur Content, der einen langfristigen Wert hat und wiederholt genutzt werden kann. Sie wissen zwar, dass Piraterie illegal ist, lassen sich davon aber nicht abhalten.
- d) Die „Faulen“ werden hauptsächlich von Kosteneinsparungen und Titelfürfügbarkeit angezogen und sind sich der Tatsache, dass Piraterie illegal ist, nicht bewusst oder sie ignorieren sie. Die VFT-Studie legt nahe, dass die Faulen und die Utilitarier ungefähr 70 Prozent der gesamten Zuschauercommunity ausmachen. Dementsprechend zeigen Initiativen, die Nutzer informieren, von legitimen Services überzeugen oder für illegal bezogene Inhalte bestrafen, den größten Nutzen.

## Können wir Piraterie aufhalten?

Die Antwort auf diese Frage lautet leider: nicht ganz. Die Geschichte der Piraterie lehrt uns, dass – solange Inhalte erstellt werden – immer irgendwer versuchen wird, das Verhältnis zwischen Angebot und Nachfrage auszunutzen. Doch es gibt einen Lichtblick. Aus verschiedenen Initiativen zur Pirateriebekämpfung auf der ganzen Welt haben wir gelernt, dass wir das Problem mit dem richtigen strategischen Ansatz auf jeden Fall minimieren können. Hierfür muss jedoch jede Instanz, die an der Wertschöpfungskette beteiligt ist, ihren Part übernehmen: von Produktion und Verbreitung bis hin zu Gesetzgebern und Aufsichtsbehörden.

### Initiativen auf Nachfrageseite

**Besserer Zugriff auf Inhalte:** Die Daten zeigen einheitlich, dass Zuschauer gestohlener Inhalte oft gleichzeitig die größten Nutzer legaler Inhalte sind. Deshalb lässt sich die Piraterie reduzieren, indem Zuschauern die Inhalte geboten werden, die sie sehen wollen – mit einem guten Streamingenerlebnis zu einem vernünftigen Preis. Eine neue Studie der Vocus-Gruppe in Neuseeland fand heraus, dass zwar elf Prozent der Zuschauer urheberrechtlich geschützte Inhalte über illegale Streams beziehen, dass jedoch 55 Prozent dieser Zuschauer den gleichen Inhalt auch über legale Services nutzen würden, wenn er dort verfügbar wäre. So hatte beispielsweise die Einführung strenger Anti-Piraterie-Gesetze in Schweden größtenteils keinen Effekt. Im Gegenteil: Die Raten gestohlener TV-Inhalte stiegen sogar nach der Einführung des Gesetzes. Erst Jahre später, mit dem Aufkommen von Netflix, nahm das Problem ab.

Leider ist das Labyrinth an Gesetzen und Kosten rund um globale Rechte ein komplexes Thema. Wir können jedoch schon jetzt sagen, dass wirklich umfassender Zugriff auf Inhalte noch sehr lange auf sich warten lassen wird. Bis vor Kurzem stellten viele OTT-Services (Over-the-Top) eher eine Defensivstrategie von Sendeanstalten oder Studios dar und wurden nicht unbedingt als große Umsatzquellen angesehen. Deshalb wurden Videoinhalte entweder hinter teuren OTT-Paywalls versteckt oder gar nicht erst verfügbar gemacht. Doch die Zeiten haben sich geändert: Mit dem Erfolg der großen SVOD-Player investieren heute viele Inhaber von Primärrechten in eigene Onlineservices. Und je weiter diese Services global eingeführt werden, desto stärker wird auch die Piraterie abnehmen.

**Informieren:** Für diejenigen, die in der Branche tätig sind, ist es natürlich völlig offensichtlich, dass Piraterie genauso wie jeder andere Diebstahl eine kriminelle Handlung ist. Außerhalb der Branche ist das Ganze jedoch nicht so klar. Piraterie wird in der breiten Bevölkerung als Kavaliersdelikt angesehen. Denn wenn alle anderen es auch machen, wirkt die Handlung auf Verbraucher irgendwann nicht mehr illegal. Leider waren bisherige Initiativen, die die Öffentlichkeit über die Folgen der Piraterie informieren sollten, nur wenig erfolgreich. Verantwortliche sollten jedoch weiterhin entsprechende Bemühungen unternehmen und die Bevölkerung daran erinnern, dass Piraterie eben kein Kavaliersdelikt, sondern eine Straftat ist und das Leben echter Menschen beeinträchtigt. Gleichzeitig sollten Werbetreibende darüber aufgeklärt werden, welche Folgen es haben kann, wenn ihre Marken mit Piratensites in Verbindung gebracht werden.

### Ein Blick in die Welt der Videopiraten

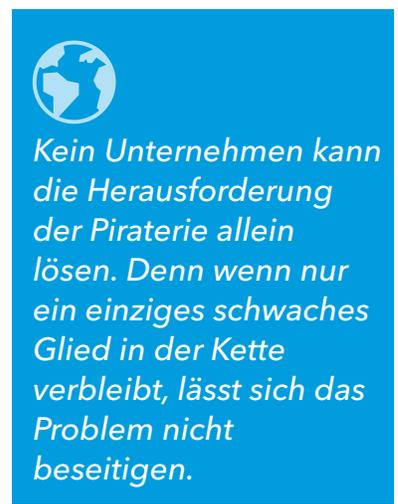
**Rechtliches:** Viele Befragte haben die fehlende Effektivität rechtlicher Maßnahmen zur Minimierung der Nachfrage betont. Abgesehen von den logistischen Herausforderungen, die es mit sich bringt, Tausende oder sogar Millionen von Personen strafrechtlich zu verfolgen, ist es aus technischer Sicht auch äußerst schwierig, die IP-Adressen zuzuordnen – insbesondere angesichts der Zunahme von Cyberlockern. Darüber hinaus gibt es heute – mit stärkerer Verbreitung von Datenschutzgesetzen – Präzedenzfälle, in denen einfach die Verbindung zwischen IP-Adressen und den angeklagten Urheberrechtsverletzern geleugnet wird. So geschehen in den US-Bundesstaaten Washington, Florida, Kalifornien und kürzlich im United States Court of Appeals für den 9. Bezirk. Derzeit laufen verschiedene innovative Fälle, die möglicherweise alternative Maßnahmen zur Verfolgung von wiederholten Zuschauern gestohlener Inhalte bieten. Besser angelegt sind rechtliche Ressourcen jedoch in der Verfolgung der eigentlichen Inhaltsdiebe und der Betreiber von Piratensites.

## Initiativen auf Angebotsseite

**Daten:** Eine offensichtliche Notwendigkeit besteht in der Entwicklung einer Standardmethodik, anhand derer sich das Ausmaß und die Folgen der Piraterie auf allen Märkten weltweit bestimmen lassen. Während unserer Recherche für dieses Whitepaper wurde deutlich, dass die vielen verschiedenen Studien zum Thema Piraterie zu einiger Verwirrung führen. Die Unterschiede zwischen den Studienmethoden lassen keine kontinuierlichen Kontextanalysen zu und führen dazu, dass Regierungen und Anbieter nicht wissen, welche Maßnahmen sie priorisieren sollen. Das ließe sich ganz einfach lösen, wenn Brancheneinrichtungen wie die Alliance for Creativity and Entertainment (ACE), die MPA oder regionale Stellen wie das EUIPO eine Führungsrolle übernehmen.

**Rechtlich und behördlich:** Im Gegensatz zur Nachfrageseite erleben wir hier einige herausragende Initiativen – sowohl national als auch global. Auf strategischer Ebene – mit verschiedenen Brancheneinrichtungen wie der ACE oder Regierungsinitiativen wie der FAPAV in Italien – erleben wir langsam organisierte Bemühungen zur Ermittlung und Verfolgung von Videopiraten und zur Schließung rechtlicher Schlußflöcher auf der ganzen Welt. Diese Bemühungen erfordern ein hohes Maß an Koordination sowie Zugang zu relevanten Daten.

**Technisch und betrieblich:** Während wir es legitimen Nutzern so einfach wie möglich machen wollen, großartige Unterhaltungserlebnisse zu genießen, wollen wir Piraten den Zugriff möglichst schwer machen. Hierfür untersuchen moderne digitale Unternehmen ihren Betrieb und ermitteln Schwachstellen in ihren Workflows – von Produktion bis Verbreitung – und implementieren geeignete Maßnahmen. Viele Rechteinhaber (gerade mit Film- und Premiumsportrechten) schreiben Dritten bereits mindestens erforderliche Betriebsstandards vor. Diese sind manchmal vertraglich vorgegeben; da sie jedoch mit Kosten und Komplexität verbunden sind, legen Rechteinhaber oftmals nur ein absolutes Mindestmaß an Schutz fest. Hierzu das Beispiel der MPA-Richtlinien: Diese sind zwar äußerst umfassend, aber nicht verbindlich. Kein Unternehmen kann die Herausforderung der Piraterie allein lösen. Denn wenn nur ein einziges schwaches Glied in der Kette verbleibt, lässt sich das Problem nicht beseitigen. Hier helfen ein 360-Grad-Ansatz gegen Piraterie und die Implementierung relevanter Verfahren nach Funktionen innerhalb des Workflows.



**Kein Unternehmen kann die Herausforderung der Piraterie allein lösen. Denn wenn nur ein einziges schwaches Glied in der Kette verbleibt, lässt sich das Problem nicht beseitigen.**

**Zusammenarbeit:** Es ist offensichtlich, dass Rechteinhaber, Verleiher und Gesetzgeber zusammenarbeiten müssen, um die Einblicke zu gewinnen und die betriebliche Koordination zu erreichen, die zur aktiven Bekämpfung der Piraterie erforderlich sind. Die Film- und Fernsehbranche ist zwar eher harten Wettbewerb gewohnt, doch die potenziellen Folgen von Piraterie sind einfach zu schwerwiegend, als dass Unternehmen allein bestehen könnten. Deshalb müssen sie auf allen Ebenen der Branche und bei allen Schritten des Prozesses zusammenarbeiten: von der Produktion und Sicherheit am Set bis hin zur Übertragung. Je mehr Unternehmen und Organisationen beteiligt sind, desto effektiver ist letztlich die Lösung. Leider gilt das auch umgekehrt: Solange es noch Schwachstellen gibt, werden diese auch ausgenutzt.

## 360-Grad-Ansatz

Nachdem wir uns die Methoden angesehen haben, mit denen die verschiedenen Piratengruppen Videos beschaffen und verbreiten, haben wir ein Framework erstellt, mit dem Kunden ihre individuelle Bedrohungslandschaft strategisch untersuchen und relevante technische Lösungen bewerten können. Bei Akamai entwickeln wir Services, um einen strategischen Anti-Piraterie-Ansatz zu schaffen, der drei Kernbereiche abdeckt: Schützen, Erkennen und Durchsetzen. Diese Bereiche lassen sich wiederum mit anderen Aktivitäten kombinieren, sodass ein effektives Anti-Piraterie-Framework entsteht.

### Schützen

**1. Schutz vor Credential Stuffing:** Wie zuvor in diesem Dokument beschrieben, nutzen viele Piraten Credential Stuffing, um sich Zuschauerdaten zu beschaffen. Für ihre Credential-Stuffing-Angriffe setzen Piraten primär automatisierte Bots auf Anmeldeseiten ein. Akamai hat bereits Medienunternehmen verschiedenster Größen bei dieser Herausforderung unterstützt und daraus viele Best Practices ableiten können. Hier unsere wichtigsten Empfehlungen:

- Programmieren Sie Anmeldeseiten oder -APIs mit OWASP. Schreiben Sie unter Einhaltung der OWASP-Best-Practices sicheren Code und führen Sie Penetrationstests auf Ihren Login-Endpoints durch.
- Nutzen Sie einen DDoS-Schutz. Hierdurch können Sie volumetrische Botnets daran hindern, Ihre Infrastruktur zu erreichen und Ihre Ressourcen zu überlasten.
- Nutzen Sie eine Bot-Management-Lösung. So können Sie durch Verifizieren von Nutzerverhalten und Gerätelemetriedaten komplexe Angriffe verhindern, bei denen Anmeldedaten missbraucht werden.

**2. Schutz vor Diebstahl aus Systemen:** Diebstähle aus internen Produktionssystemen, digitalen Speichern oder der Public Cloud werden in der Branche nicht oft bekannt gegeben. Wir haben jedoch herausgefunden, dass es sich hierbei um eine wichtige Quelle der Piraterie handelt. Der Diebstahl von Video-Assets lässt sich grob in folgende Kategorien aufteilen:

- Direkte Hacks oder Man-in-the-Middle-Angriffe durch Piraten
- Diebstahl durch Mitarbeiter oder Freiberufler
- Abgreifen eindeutiger System-IDs, wie z. B. Passwörter

Es gibt zahlreiche Technologien, mit denen Unternehmen, die an Produktions- und Vordistributionsworkflows beteiligt sind, das Risiko minimieren können. Und im Grunde setzen sie alle auf das Konzept von Zero Trust. In einer Branche, die stets ein hohes Maß an Vertrauen innerhalb ihres Ökosystems vorausgesetzt hat, klingt das erst einmal nach einer krassen Veränderung. Tatsache ist jedoch, dass die Normen und Maßnahmen, die die Mediengemeinschaft bisher zusammengehalten haben, in der digitalen Welt nicht mehr existieren.

Zero Trust ist ein Framework, mit dem Unternehmen ihre Kern-IT und ihre Medienproduktionssysteme transformieren und klassische, veraltete Netzwerksicherheitssysteme ersetzen können. Das Framework basiert auf der Idee, dass es kein internes Netzwerk mehr gibt, in dem Personen oder Geräten vertraut werden könnte. Die Kernkomponenten eines Zero-Trust-Frameworks umfassen: sicheren Zugriff auf alle Ressourcen (unabhängig von Standort oder Hostmodell); die Durchsetzung einer strengen Zugriffskontrollstrategie basierend auf dem Prinzip der geringstmöglichen Berechtigungen; sowie die Untersuchung und Protokollierung des gesamten Traffics, um verdächtige Aktivitäten zu erkennen. In diesem Framework haben nur authentifizierte und autorisierte Nutzer und Geräte Zugriff auf Anwendungen und Daten. Gleichzeitig werden diese Anwendungen und Nutzer vor hochentwickelten Bedrohungen im Internet geschützt.

Unternehmen stehen zahlreiche Komponenten zur Verfügung, um ein Zero-Trust-Framework zu implementieren. Ein wichtiger Punkt ist hierbei der sichere Mitarbeiter- und Freiberuflerzugriff auf Produktionsanwendungen und Medienspeichersysteme. Aufgrund der hohen Fluktuation bei den beteiligten Arbeitskräften stehen Medienunternehmen vor einmaligen Herausforderungen bei Bereitstellung und Entzug von Systemzugriff – manchmal vom einen Tag auf den anderen. Mit Services wie Akamai Enterprise Application Access lassen sich schnell und einfach Nutzerberechtigungen für spezifische Anwendungen gewähren, basierend auf der Identität und dem Sicherheitskontext der Nutzer und ihrer Geräte. Wichtig ist: Hierbei erhält kein Nutzer jemals Zugang zum gesamten Unternehmensnetzwerk.

Ein weiterer Kernbereich von Zero Trust ist die Implementierung von Systemen, die gezielte Bedrohungen wie Malware, Ransomware oder Phishing proaktiv erkennen und blockieren können. Denn diese Tools werden von Piraten gern für Man-in-the-Middle-Angriffe eingesetzt. Akamai Enterprise Threat Protector ist beispielsweise ein Secure Web Gateway, das Echtzeit-Sicherheitsinformationen verwendet und neben Malware, Ransomware und Phishing auch DNS-basierte Datenextraktionen erkennt und blockiert.

**Schutz vor Geo- und IP-Rechtsverletzungen:** Eine weitere Methode zur Beschaffung von Inhalten ist der Einsatz von VPN-Technologien, um das Ursprungsland und die IP-Adresse der Piraten zu verbergen. Diese Aktivität folgt in der Regel auf die erfolgreiche Beschaffung von Daten legitimer Abonnenten. Nachdem die Daten beschafft wurden, können Piraten ihren geografischen Standort und ihre IP-Adresse verschleiern, um Inhalte an mehrere Standorte zu streamen. Dieser Prozess wird als Restreaming bezeichnet. Die starke Verbreitung von VPN-Services bedeutet auch, dass die Gruppe der „faulen“ Piraten ganz leicht auf geografisch beschränkte Inhalte zugreifen kann, wie z. B. Zuschauer aus Europa, die eine spezielle US-amerikanische TV-Serie sehen wollen. Zum Schutz vor solchen Aktivitäten helfen Mechanismen wie Proxy-Erkennungstechnologien. Akamai Enhanced Proxy Detection blockiert auf intelligente Weise Anfragen, die mit anonymen Proxys oder VPN-Services in Verbindung stehen, direkt an der Edge.

**Schutz vor unrechtmäßiger Wiedergabe:** Hierbei handelt es sich bei Weitem um die beliebteste Taktik gegen Piraterie. Sie lässt sich über eine Reihe verschiedener Maßnahmen erreichen – am häufigsten kommt hierbei Digital Rights Management (DRM) zum Einsatz.

Zusammengefasst bezieht sich DRM auf die Tools, Standards und Systeme, die zur Beschränkung geschützter digitaler Inhalte und zur Verhinderung der unautorisierten Verbreitung eingesetzt werden. Es handelt sich also nicht wirklich um eine einzige Technologie. Bei nicht kritischen Assets setzen einige Anbieter auf einfache Verschlüsselung. Hierbei werden Zuschauer daran gehindert, Kopien von Videos anzufertigen, indem der Inhalt in einem Code geschrieben wird, der nur von Geräten und Software mit entsprechendem Key zum Entschlüsseln des Codes gelesen werden kann. Diese Methode bietet durch die Notwendigkeit eines Schlüssels zumindest oberflächlichen Schutz. Die Keys werden in der Regel von HTTP-Servern bereitgestellt und können kopiert und weitergegeben werden. Verschlüsselung reicht also nicht aus, um wertvollere Inhalte zu schützen. Fortschrittlichere DRM-Technologien verarbeiten die Schlüsselkommunikation über ein spezielles Modul, das mit einem Sicherheitsfrage-und-Antwort-System arbeitet. Diese Kommunikation wird verschlüsselt, damit der Entschlüsselungskey niemals offen lesbar ist, selbst wenn er gehackt wird. Moderne DRM-Technologien bieten darüber hinaus oft die Möglichkeit, Geschäftsregeln hinzuzufügen, die definieren, wann und wie die Schlüssel auf den verschiedenen Geräten verwendet werden können. Hierbei werden Kriterien wie Standort, Geräteregistrierung und zeitbasierte Regeln überprüft. Wie alle Technologien bringt jedoch leider auch DRM einige Herausforderungen mit sich.

- a) Die erste lautet Komplexität. Bei diesem Thema wollen wir nicht allzu sehr ins Detail gehen, deshalb hier ein kurzer Überblick: Unternehmen, die eine umfassende DRM-Strategie implementieren wollen, müssen verschiedene Technologien unterstützen, darunter mindestens Apple FairPlay, Google Widevine und Microsoft PlayReady. Nur so können sie eine ausreichende Abdeckung der potenziellen Browser, Geräte und Betriebssysteme erreichen, die auf dem Markt verfügbar sind. Diese verschiedenen Systeme führen jedoch auch zu mehr Kosten und Komplexität im Workflow. Über eine Spezifikation namens Common Media Application Format (CMAF) verschiebt sich der DRM-Markt derzeit hin zu einem einzigen Format für verschlüsselte Dateien, das alle drei Technologien unterstützt. Ältere Geräte werden jedoch bisher nicht unterstützt.
- b) Die zweite Herausforderung ist die Abhängigkeit von Drittanbietersystemen für den DRM-Betrieb. Wenn diese Systeme gehackt werden oder einen DoS-Angriff erleiden, wird das Zuschauererlebnis beeinträchtigt.
- c) Der finale Bereich wird von DRM-Gegnern als Achillesferse der Technologie angesehen. DRM kann Inhalte nicht schützen, wenn sie nicht mehr verschlüsselt sind, wie es beispielsweise bei Bildschirmaufzeichnungen der Fall ist. Es gibt zahlreiche Fälle, in denen Spezialisten versuchen, die verschiedenen DRM-Technologien zu umgehen, um so Schwachstellen zu finden. Dass technisch versierte und oftmals obsessive Piraten Wege finden, um DRM-Maßnahmen zu umgehen, sollte keine große Überraschung darstellen. Das Ganze ist jedoch kein Grund, DRM aus der Strategie zu werfen.



*Sicherer Mitarbeiter- und Freiberuflerzugriff auf Produktionsanwendungen und Medienspeichersysteme ist ein wichtiger Faktor.*

Viele Rechteinhaber – gerade solche mit wertvollen Sport- und Filmrechten – schreiben Verleihen die Implementierung von DRM-Schutzmaßnahmen vor. Die Spezifikationen unterscheiden sich hierbei je nach Inhaber: von allgemeinen Richtlinien bis hin zu exakten Anforderungen. Für Verleihe, die DRM schon im Paketierungsprozess implementieren wollen, ist es oftmals nützlich, mit einem Cloudanbieter zusammenzuarbeiten, der die Komplexität abfangen kann. Akamai bietet beispielsweise einen integrierten Ursprungsspeicher für On-Demand-Inhalte. Dieser umfasst die Verarbeitungsfunktionen verschiedener Provider, wie z. B. Bitmovin und Encoding.com, die DRM nahezu in Echtzeit implementieren können. Als Alternative zu DRM setzen immer mehr Unternehmen auf die Vorteile einer Kombination aus Verschlüsselung und Wasserzeichen. Diese Methode bietet erhebliche Vorteile in Sachen Verarbeitungskosten und Zuschauererlebnis, erreicht jedoch ebenfalls eine zuverlässige Form von Wiedergabeschutz.

## Erkennen

Wie bei jeder Art von Diebstahl ist der Erfolg von Schutzmaßnahmen nie garantiert. Deshalb ist auch die Erkennung von Rechtsverletzungen entscheidend. Es gibt zahlreiche Methoden, um betrügerische Aktivitäten von Piraten nahezu in Echtzeit zu erkennen.

**Fingerprinting:** Diese Methode bietet die Möglichkeit, Videoinhalte ohne Änderung der Originalmedien zu erkennen. Hierbei kommen Tools zum Einsatz, die Attribute von Videodateien erkennen, extrahieren und darstellen, damit jedes Video mit einem eindeutigen „Fingerabdruck“ identifiziert werden kann, z. B. in Filesharing-Netzwerken. Ein solcher Fingerabdruck kann zwischen verschiedenen Kopien desselben Titels unterscheiden und damit erkennen, wessen Video illegal kopiert wurde. Entsprechend kommt die Technologie bei Services wie YouTube Content ID zum Einsatz, um zu erkennen, wann urheberrechtlich geschütztes Material von Konten hochgeladen wird, denen die erforderlichen Rechte zur Weiterverbreitung fehlen. Darüber hinaus können Unternehmen mithilfe von Fingerprinting Informationen dazu erhalten, wie weit Piraterie unter ihren Inhalten verbreitet ist, bevor sie eine zuverlässige Strategie einrichten.

**Watermarking:** Hierbei handelt es sich um die am weitesten verbreitete Form der Piraterie-Erkennung. Zwar können Wasserzeichen die Piraterie nicht direkt aufhalten, doch mit ihnen können Serviceanbieter Videodiebstahl erkennen, die Beteiligten identifizieren und dagegen vorgehen. Im Grunde handelt es sich bei Videowasserzeichen um ein Muster von Bits, das in eine Videodatei integriert wird und für das menschliche Auge nicht zu erkennen ist. Dieses Muster lässt sich auch nicht aus dem Video entfernen. Indem diese Daten mit der Identität des Zuschauers verbunden werden, können Piraten verfolgt werden, die Inhalte entschlüsseln, kopieren und illegal verbreiten.

Derzeit kommen drei Methoden für Videowasserzeichen zum Einsatz: Bitstream-Modifikation, Watermarking mit A/B-Varianten und clientseitiges Watermarking.

**Bitstream-Modifikation** beinhaltet die Änderung ausgewählter Bereiche eines Bildes, sodass zwar die Videoqualität beibehalten wird, aber der Zuschauer und seine Sitzung identifiziert werden können. Diese Methode ist zuverlässig, verursacht jedoch einen erheblichen Computing-Overhead und steigert die Latenz des Systems, wodurch sie für Livesysteme ungeeignet ist.

**Watermarking mit A/B-Varianten** wurde für den OTT-Sektor entwickelt. Hierbei werden zwei identische Videostreams erstellt, mit Wasserzeichen versehen und daraufhin clientseitig oder über CDN-Edge-Verarbeitung ineinander verflochten, um eine eindeutige Identifikation zu ermöglichen. Diese Methode ist zwar zuverlässig und kostengünstig, da aber die Identifikationsabfolge lang dauern kann, ist sie für Situationen, die eine schnelle Wasserzeichenextraktion erfordern, nicht geeignet.

**Clientseitiges Watermarking** wird aufgrund der schnellen Wasserzeichenextraktion und der möglichen Bereitstellung auf älteren Plattformen bevorzugt. Hierbei wird über den Videostream auf dem Clientgerät ein grafisches Overlay gelegt, das unsichtbar gemacht werden kann. Das Wasserzeichen wird also erst angewendet, wenn es den Client erreicht, weshalb der Inhalt zusätzlich auf dem Übertragungsweg geschützt werden muss. Darüber hinaus müssen Verleiher hierfür die Bereitstellung von SDKs für OTT-Geräte in Erwägung ziehen, was den betrieblichen Overhead steigern kann.

Es gibt zahlreiche Möglichkeiten für Wasserzeichen, die sämtliche Anwendungsfälle abdecken. Ein wichtiges Element jeder Watermarking-Strategie ist jedoch eine geeignete Überwachung, damit die richtigen Durchsetzungstechniken gegen Piraten eingesetzt werden können. Viele Provider von Anti-Piraterie-Technologie bieten Managed Services für die Überwachung an. Alternativ können sich Unternehmen von entsprechenden Anbietern beraten lassen, um interne Funktionen zu entwickeln.

Akamai arbeitet mit großen Watermarking-Providern zusammen, um Kunden eine optimale Lösung bereitzustellen, die im Rahmen der allgemeinen Anti-Piraterie-Strategie verfügbar und darin integriert ist.

**Streamprotokoll-Identifikation:** Eine weitere Art der Erkennung ist die Echtzeituntersuchung der Protokolle von Distributionspartnern, wie z. B. CDNs. So lassen sich beispielsweise illegale Livestreams ermitteln. In diesem Szenario wird durch gründliche Protokolluntersuchung eine Echtzeitübersicht betrügerischer Aktivitäten bereitgestellt – basierend auf autorisierten und nicht autorisierten IP-Adressen. Der Vorteil entsprechender Lösungen, wie z. B. Akamai Stream Protector: Die Funktion kann je nach Situation schnell ein- und ausgeschaltet werden und es können spezifische Regeln durchgesetzt werden. Hierzu ein Beispiel: Eine Sendeanstalt verfügt für kurze Zeit über wertvolle Sportrechte, will aber nicht in Watermarking-Technologie investieren. Deshalb nutzt sie die Streamprotokoll-Identifikation, um ein ähnliches Maß an Schutz zu bieten, ohne den Bereitstellungsworkflow oder die Technologiekosten zu beeinträchtigen. Der Nachteil dieser Technologie liegt darin, dass sie nur mit einem Distributionspartner verwendet werden kann, was in Umgebungen mit mehreren CDNs eine Herausforderung darstellt.

## Durchsetzen

Wenn betrügerische Aktivität erkannt wird, ist es wichtig, auf geeignete Weise zu reagieren. Je nach Strategie stehen Ihnen unterschiedliche Optionen zur Verfügung:

**Zugriffssperre:** Wenn bei Ihren Video-Assets Zeit eine Rolle spielt, wie z. B. bei Sport- oder anderen Live-Events, dann sollten Sie dem Bereitsteller des illegalen Streams schnellstmöglich den Zugriff entziehen. Hierzu gibt es verschiedene Methoden. Sie können sich zum Beispiel mit Ihrem Distributionserviceanbieter kurzschließen, relevante Details austauschen und Streamingaktivitäten von der entsprechenden IP-Adresse blockieren. Wenn entsprechende Betriebsprozesse vorhanden sind, lässt sich das Ganze in relativ kurzer Zeit bewerkstelligen. Es gibt jedoch verschiedene Szenarien, in denen „relativ kurz“ nicht ausreicht, wie z. B. bei Sportereignissen

oder wenn die Verbreitung des gestohlenen Inhalts viral gehen könnte. Deshalb bietet Akamai einen Service an, mit dem Streams in Echtzeit und ohne menschliche Interaktion gesperrt werden können. Diese Technik hat sich gerade in Fällen, in denen die Piraterieüberwachung über Wasserzeichen oder Streamprotokoll-Identifikation erfolgt, als äußerst effektiv erwiesen.

## Ein Blick in die Welt der Videopiraten



*Mit geeigneter Überwachung können die richtigen Durchsetzungstechniken gegen Piraten eingesetzt werden.*

**Stream-Modifikation:** In Szenarien, in denen Zeit eine weniger wichtige Rolle spielt, können Anbieter die illegalen Streams modifizieren, indem sie legale Inhalte mit alternativem Inhalt bereitstellen (derzeit ist *Big Buck Bunny* beliebt) oder die Streamqualität reduzieren. Diese Ansatz hat den Vorteil, dass der Bereitsteller des Streams nicht direkt erkennt, dass er erkannt wurde, und daher die Streamquelle nicht wechselt.

**Echtzeitnachrichten:** Wie zuvor zum Profil des „faulen“ Piraten beschrieben, fühlt sich diese Gruppe durch die Anonymität des Internets geschützt. Unternehmen wie VFT können Zuschauer von illegalen Livestreams auf Social-Media-Plattformen erkennen und sie direkt anschreiben. Mit dieser Form der Durchsetzung können Anbieter ihre Reaktion stufenweise anpassen. Sie können beispielsweise zu Beginn auf die legalen Streams verweisen und bei wiederholten Vergehen rechtliche Hinweise einblenden.

Um die allgemeine Aufklärung über das Thema zu unterstützen, treten immer mehr und immer fortschrittlichere Echtzeit-Nachrichtenplattformen auf den Plan, die Nutzer gestohlener Inhalte ansprechen können. Mit den richtigen Anti-Piraterie-Services können Betreiber Zuschauer ermitteln, die illegale Streams nutzen, und sie dazu anhalten, zu legalen Services zu wechseln – mit freundlichen oder strengen Gegenmaßnahmen. Sie können beispielsweise Nutzer über die Folgen ihrer Aktionen informieren, sie mit speziellen Angeboten zu legalen Alternativen locken oder hart durchgreifen, indem sie die Strafverfolgungsbehörden miteinbeziehen. Wichtig ist hierbei, Zuschauern das Gefühl der Anonymität zu nehmen und sie aktiv aufzuklären.

## Fazit

Videopiraterie im Internet ist ein äußerst komplexes Problem mit vielen Facetten. Und leider hat dieses Problem das Potenzial, der Medienbranche langfristig großen Schaden zuzufügen. Zahlreiche Studien legen nahe, dass Piraterie erhebliche finanzielle Schäden verursacht und – was noch wichtiger ist – potenziell die globalen Lizenzierungsmodelle beeinträchtigen könnte.

Bisher war die Reaktion der Branche eher verhalten. Sendeanstalten, Pay-TV-Betreiber und Brancheneinrichtungen haben beim Kampf gegen Piraterie nur wenig zusammengearbeitet und die Last lieber allein getragen. Ein Analyst beschreibt die Situation wie folgt: „Wir befinden uns in einer Early-Adopter-Phase. Es liegt noch viel Arbeit vor uns.“ Immer mehr Anbieter erkennen die Gefahr und die meisten Top-Videoproduzenten und -Betreiber haben mittlerweile spezielle Teams aufgebaut, um Piraterie näher zu untersuchen, die eigene Situation zu bewerten und geeignete Anti-Piraterie-Strategien zu implementieren. Wie in diesem Whitepaper beschrieben wird jedoch der Kampf ohne ein gewisses Maß an gemeinsamen betrieblichen Prozessen und Koordination innerhalb der Branche äußerst hart. Und auch die Unterstützung von Regierungen, Aufsichtsbehörden und Servicegebern ist für den Erfolg entscheidend. Wie in jedem Kampf reicht ein schwaches Glied aus, um die gesamte Kette zu gefährden.

In diesem Whitepaper wurden verschiedene unmittelbare Anforderungen beschrieben, die für den Kampf der Branche gegen Piraterie essenziell sind. Hierzu zählen zum einen einheitliche Piraterie-Datenpunkte, damit Führungskräfte und die breitere Branche die Bedrohungen verstehen, und zum anderen kontinuierliche Aufklärung der Öffentlichkeit über die Folgen der Piraterie für die Beschäftigung und nationale Branchen. Darüber hinaus müssen Anti-Piraterie-Provider und Serviceanbieter gemeinsam gewährleisten, dass technische Lösungen effizient integriert werden können. Und zu guter Letzt müssen Rechteinhaber in der gesamten Branche eine Führungsrolle in der Verarbeitung und Verbreitung von geschützten Inhalten übernehmen.

Die gute Nachricht ist, dass viele dieser Punkte bereits umgesetzt werden. Das EUIPO stellt beispielsweise klare Datenpunkte zum Umfang und zu den Folgen der Piraterie in der Europäischen Union bereit - mit einer Methodik, die einfach von anderen Regionen übernommen werden kann. Nationale Regierungen müssen sich des Problems bewusst werden. Und genau hier können klarere Informationen über die Folgen der Piraterie dafür sorgen, dass wir bald strengere Gesetze erwarten können. Anbieter versuchen immer häufiger, ihre Stärken zu kombinieren. Akamai stellt beispielsweise nicht nur sein Know-how zur Cybersicherheit bereit, sondern arbeitet auch mit allen führenden Watermarking-Unternehmen zusammen, um zu gewährleisten, dass Piraten - wenn sie einmal erkannt wurden - sofort blockiert werden können. Und auch Rechteinhaber schreiben zusehends Mindeststandards für den Inhaltsschutz in technischen Workflows vor. Derzeit handelt es sich hierbei noch um einzelne Fälle oder „Empfehlungen“ (wie bei der MPA), doch wir gehen davon aus, dass entsprechende Standards in Zukunft für Deals mit Rechteinhabern zwingend erforderlich sein werden.

Mit entsprechenden Initiativen können wir das Problem minimieren, finanzielle Verluste reduzieren, Beschäftigungsmöglichkeiten schützen und die Lizenzierung auf dem globalen Markt fördern.



*Akamai arbeitet mit allen führenden Watermarking-Unternehmen zusammen, um zu gewährleisten, dass Piraten - wenn sie einmal erkannt wurden - sofort blockiert werden können.*

## QUELLENANGABEN

- Asia Video Industry Association. The Asia Video Industry Report. 2019.
- Bevir. Cost of online piracy to hit \$52bn. 2017. Abgerufen unter <https://www.ibt.com/publish/cost-of-online-piracy-to-hit-52bn/2509.article>
- Blackburn u. a. Impacts of Digital Video Piracy on the U.S. Economy. 2019.
- Coberly. Streaming services are 'killing' piracy. Abgerufen unter <https://www.techspot.com/news/78977-streaming-services-killing-piracy-new-zealand-study-claims.html>
- CustosTech. The Economics of Digital Piracy. 2014.
- Daly. Pirates of the Multiplex. Abgerufen unter <https://www.vanityfair.com/news/2007/03/piratebay200703>
- Decary, Morselli, Langlois. A Study of Social Organisation and Recognition Among Warez Hackers. 2012.
- Digital Citizens Alliance. Fishing in the Piracy Stream. Abgerufen unter [https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA\\_Fishing\\_in\\_the\\_Piracy\\_Stream\\_v6.pdf](https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf)
- Enigmmax. Interview with a Warez Scene Releaser. 2007. Abgerufen unter <https://torrentfreak.com/interview-with-a-warez-scene-releaser/>
- Europäische Kommission. Estimating displacement rates of copyrighted content in the EU. Mai 2015.
- Amt der Europäischen Union für geistiges Eigentum. Trends in Digital Copyright Infringement in the European Union. 2018.
- Amt der Europäischen Union für geistiges Eigentum. Illegal IPTV in the European Union. 2019.
- FACT. Cracking Down on Digital Piracy. 2017.
- Feldman. Artikel zur Nutzung von Streamingsservices. 2017. Abgerufen unter <https://youngov.co.uk/topics/politics/articles-reports/2017/04/20/almost-five-million-britons-use-illegal-tv-streams>
- FriendsMTS. Comparing subscriber watermarking technologies for premium pay TV content. 2019.
- Frontier Economics. The Economic Impacts of Counterfeiting and Piracy - Report prepared for BASCAP and INTA. 2017.
- Granados. Report: Millions Illegally Live-Streamed El Clasico. 2015. Abgerufen unter <https://www.forbes.com/sites/nelsongranados/2016/12/05/sports-industry-alert-millions-illegally-live-streamed-biggest-spanish-soccer-rivalry/#3544c3f37147>
- Greenburg. The Economics of Video Piracy. 2015. <https://pitjournal.unc.edu/article/economics-video-piracy>

D. Iboiola, B. Steer, A. Garcia-Recuero, G. Stringhini, S. Uhlig und G. Tyson. *Movie Pirates of the Caribbean: Exploring Illegal Streaming Cyberlockers*. 2018.

Intellectual Property Office. *Online Copyright Infringement Tracker*. 2018.

Jarnikov u. a. *A Watermarking System for Adaptive Streaming*. 2014.

Jones, Foo. *Analyzing the Modern OTT Piracy Video Ecosystem*. SCTE•ISBE. 2018.

Joost Poort u. a. *Institut für Informationsrecht, Universität Amsterdam. Global Online Piracy Study*. Juli 2018.

Kan. *Pirating 'Game of Thrones'? That File Is Probably Malware*. 2019. Abgerufen unter <https://mashable.com/article/pirating-game-of-thrones-malware/?europe>

T. Lee. *Texas-Size Sophistry*. 2006. Abgerufen unter <http://techliberation.com/2006/10/01/texas-size-sophistry/>

S. Liebowitz. „The impact of internet piracy on sales and revenues of copyright owners“ – eine kürzere Version von „Internet piracy: the estimated impact on sales“ in „Handbook on the Digital Creative Economy“ von Ruth Towse und Christian Handke, Edward Elgar. 2013.

J. Mick. *Nearly half of Americans pirate casually, but pirates purchase more legal content*. 21. Januar 2013. Abgerufen unter <http://www.dailytech.com/Nearly+Half+of+Americans+Pirate+Casually+But+Pirates+Purchase+More+Legal+Content/article29702.htm>

Motion Picture Association of America. *The Economic Contribution of the Motion Picture & Television Industry to the United States*. November 2018.

MPA Content Security Program. *Content Security Best Practices Common Guidelines*. Motion Picture Association. 2019.

MUSO. *Measuring ROI in content protection*. 2020.

Nordic Content Protection Group. *Annual Report, 2020*.

Parks Associates. *Video Piracy: Ecosystem, Risks, and Impact*. 2019.

P. Tassi. 15. April 2014. *'Game of Thrones' Sets Piracy World Record, But Does HBO Care?* Abgerufen unter <http://www.forbes.com/sites/insertcoin/2014/04/15/game-of-thrones-sets-piracy-world-record-but-does-hbo-care>

J. Sanchez. 3. Januar 2012. *How Copyright Industries Con Congress*. Abgerufen unter <http://www.cato.org/blog/how-copyright-industries-con-congress>

Sandvine. *Video and Television Piracy*. 2019.

Schonfeld. *The Pirate Bay Makes \$4 Million A Year*. 2008. Abgerufen unter <https://techcrunch.com/2008/01/31/the-pirate-bay-makes-4-million-a-year-on-illegal-p2p-file-sharing-says-prosecutor/>

Sulleyman. *Pirate Treasure: How Criminals Make Millions From Illegal Streaming*. 2017. Abgerufen unter <https://www.independent.co.uk/life-style/gadgets-and-tech/news/piracy-streaming-illegal-feeds-how-criminals-make-money-a7954026.html>

Techspot. *Streaming services are 'killing' piracy*. Untersuchung der Vocus-Gruppe. 2019. Abgerufen unter <https://www.techspot.com/news/78977-streaming-services-killing-piracy-new-zealand-study-claims.html>

Torrentfreak. *Making Money from Movie Streaming Sites, an Insiders Story*. 2013. Abgerufen unter <https://torrentfreak.com/making-money-from-movie-streaming-sites-an-insiders-story-131019/>

VFT. *Pirate Persona Whitepaper*. 2014.

B. Walters. *Interview mit Helen Mirren*. Time Out London. Abgerufen unter <http://www.timeout.com/london/film/interview-with-helen-mirren>



Akamai stellt sichere digitale Erlebnisse für die größten Unternehmen der Welt bereit. Die Intelligent Edge Platform umgibt alles – vom Unternehmen bis zur Cloud –, damit unsere Kunden und ihre Unternehmen schnell, intelligent und sicher agieren können. Führende Marken weltweit setzen auf die agilen Lösungen von Akamai, um die Performance ihrer Multi-Cloud-Architekturen zu optimieren. Akamai bietet Schutz vor Angriffen und Bedrohungen, beschleunigt Entscheidungen und Anwendungen und liefert herausragende Online-Erlebnisse. Das Akamai-Portfolio für Website- und Anwendungsperformance, Cloudsicherheit, Unternehmenszugriff und Videobereitstellung wird durch einen herausragenden Kundenservice, Analysen und Rund-um-die-Uhr-Überwachung ergänzt. Warum weltweit führende Unternehmen auf Akamai vertrauen, erfahren Sie unter [www.akamai.com](http://www.akamai.com), im Blog [blogs.akamai.com](http://blogs.akamai.com) oder auf Twitter unter [@Akamai](https://twitter.com/Akamai). Unsere globalen Standorte finden Sie unter [www.akamai.com/locations](http://www.akamai.com/locations). Veröffentlicht: Juli 2020.