WHITEPAPER

Schutz der Bank of OTT

Akamai

Einführung

Das Problem der Videopiraterie ist nicht neu: Schon seit Beginn der professionellen Filmproduktion versuchen Kriminelle, mit der illegalen Weitergabe von Privateigentum – hier in Form von Urheberrechtsverletzungen – schnell zu 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 getarnte Prüfer damit beauftragte, diese Kinobesitzer auf frischer Tat zu ertappen. Das „Teilen" von Filmen über das Internet machte die digitale Verteilung jedoch besonders einfach und effektiv. Tausende von Raubkopien ließen sich sofort an Millionen von Zuschauern verteilen.

Heute nutzen Videopiraten eine Vielzahl von Angriffsvektoren, um Inhalte abzurufen und zu verbreiten. Gängige Taktiken sind Credential Stuffing (um die Daten von Zuschauern zu erfassen und legitime Konten zu kapern) oder die Umleitung linearer Stream-Kanäle in einer Form, die vom Fernsehen nicht zu unterscheiden ist. Gewerbliche Videopiraten bieten Kunden oft einfache Bedienungsmöglichkeiten, Kundenservice und eine Reihe flexibler Geschäftsmodelle.

Vor diesem Hintergrund werden wir uns gemeinsam mit der Piraterie beschäftigen und nach Wegen suchen, wie wir uns mithilfe eines strategischen Frameworks zur Wehr setzen können.

Schätzungen zufolge greifen 13,7 Millionen Menschen in den EU-Ländern regelmäßig auf illegale Piratendienste zu (laut EUIPO 2019), wobei Großbritannien (2,4 Mio.) und Frankreich (2,3 Mio.) jeweils die größten Zahlen illegaler Nutzung aufweisen. Die jährlichen Einnahmen durch Piraterie in der EU werden auf 1 Milliarde Euro (EUIPO 2019) geschätzt. In Nordamerika greifen Schätzungen zufolge mehr als 12,5 Millionen US-Haushalte auf Inhalte von Videopiraten zu (Parks Associates 2019) und im asiatisch-pazifischen Raum ist das Problem möglicherweise noch viel ausgeprägter. In Hongkong hat eine AVIA-Studie 2019 beispielsweise ergeben, dass 24 % der Verbraucher Internet-Streaming-Geräte für den Zugriff auf raubkopierte Kanäle verwenden. Dieser Wert steigt in den Philippinen auf 28 %, in Taiwan auf 34 % und in Thailand auf 45 %. Trotz branchenweiter Bemühungen können wir sehen, dass Videopiraterie weltweit unverändert ein ernsthaftes Problem ist. Die Auswirkungen sind in der gesamten Branche spürbar, was finanzielle Verluste und Stellenverluste zur Folge hat, und wir erkennen auch Anzeichen für eine Beeinträchtigung der Lizenzierung.

40 bis 97,1 Milliarden USD

Geschätzte Verluste in der Filmindustrie durch Raubkopien von Videos

39,3 bis 95,4 Milliarden USD

Geschätzte Verluste in der TV-Branche aufgrund von Raubkopien

Absolute Zahlen sind aufgrund der Komplexität des Themas schwer zu ermitteln. In einem von der US-Handelskammer in Auftrag gegebenen Bericht werden die finanziellen Verluste für die Filmindustrie auf 40 bis 97,1 Milliarden USD geschätzt, und für die TV-Branche auf 39,3 bis 95,4 Milliarden USD (NERA Consulting 2019). Darin sind Einkommensverluste für den Staat durch Steuern noch nicht enthalten.

Die TV- und Filmindustrie stellt Millionen von Jobs, von Set-Designern, Make-up-Künstlern und Musikern bis hin zu Produzenten und Regisseuren – und diese werden durch Piraterie gefährdet. In ihrem Bericht von 2019 zu den Folgen der Videopiraterie auf die US-Wirtschaft kamen Blackburn, Eisenach und Harrison zu dem Schluss, dass in diesem Jahr in den USA zwischen 230.000 und 560.000 Stellen aufgrund von Piraterieaktivitäten verloren gingen.

Wir haben außerdem bereits erste Anzeichen dafür erlebt, dass Piraterie die Lizenzierung beeinträchtigt. Und da die Lizenzierung das Herzblut der Kreativbranche darstellt, ist dieses strategische Problem besonders schädlich. Einfach ausgedrückt: Warum sollten potenzielle Verleihe erhebliche Summen für Rechte bezahlen, wenn Inhalte einfach und kostenlos auf Pirateriesseiten verfügbar sind? 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, und das Geschäftsmodell muss neu durchdacht werden". Er betont, dass der Wert der Rechte für sein Unternehmen auf dem Maß an Exklusivität basiert. Auch Jason Blum, Oscar-Nominierter und Emmy-Award-Gewinner, beschreibt die direkten Folgen der Piraterie auf die Bereitstellung der Mittel für innovative und gewagtere Filme. Er ist der Meinung, dass irgendwann in nicht allzu ferner Zukunft die Zahlen nicht mehr tragbar sein werden und Studios entsprechende Produktionen streichen müssen.

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. Obwohl es den Umständen entsprechend schwierig ist, Erkenntnisse zu gewinnen, wissen wir, dass wir es mit einer komplexen Reihe von Gruppen und Untergruppen zu tun haben, von denen jede ihre eigenen Antriebsfaktoren und technischen Kompetenzen hat.

Die Releasegruppen

Mitglieder sehen sich als Revolutionäre im Kampf gegen Großkonzerne. Die Mitgliedschaft bei Upload-Sites 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. FACT beschreibt die Struktur als „komplexe, anspruchsvolle und gut organisierte Gruppen im Hacker-Stil, die vermutlich an anderen Arten von Cyberkriminalität beteiligt sind".

Es gibt eine komplexe Struktur von Piratengruppen und Untergruppen, die jeweils eigene Antriebsfaktoren und Kompetenzen haben.

Die Sitebetreiber

Sie verwalten Piratenvideosites, darunter Torrent-Sites wie Pirate Bay oder Streaming-Sites wie TeaTV. 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 zwischen den beiden bestehen. Die Betreiber verdienen mit Sicherheit Geld mit dem Prozess und betreiben oft mehrere „gespiegelte" Websites, sodass sie, wenn eine Site von den Behörden geschlossen wird, weiterhin online bleiben und Geld verdienen können.

Die Großhändler für Streaminggeräte

Die wachsende Verbreitung dieser Geräte, insbesondere Kodi, bietet opportunistischen Kriminellen einen relativ stetigen und vorhersehbaren Einnahmestrom. Großhändler importieren die Boxen über ganz legale Kanäle oder kriminelle Netzwerke und modifizieren sie mit illegaler Software, die dann online verkauft werden kann.

Die Social-Media-Piraten

Oft werden Inhalte über soziale Medien verbreitet. Die Teilnehmer dieser Gruppe sind sich der Tatsache, dass Piraterie illegal ist, weniger bewusst oder ihr gegenüber gleichgültig. Sie reagieren mit ihrem Handeln entweder auf die Kosten bestimmter Inhaltsgenres oder die Unlust, Abonnements abzuschließen.

Wie beschaffen Piraten Inhalte?

Es gibt viele Methoden für Piraten, Inhalte zu stehlen, weil es zahlreiche Schwächen in der Wertschöpfungskette gibt, die ausgenutzt werden können. Wir können die am häufigsten verwendeten Methoden basierend auf dem Anwendungsfall gruppieren.

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. Dies wird erreicht durch:

- Manipulation von Videowiedergabe-Software oder des Android-Betriebssystems
- Anfertigen von Bildschirmaufnahmen während der Wiedergabe mit einem mobilen Gerät
- Abfangen verschlüsselter Videosignale mit HDCP-Strippern, die an Set-Top-Boxen angeschlossen werden
- Credential-Stuffing-Angriffe, um auf Anmeldedaten legitimer Nutzer zuzugreifen und diese zu verwenden
- Weiterleiten von Videos über die Grenzen des jeweiligen Marktes über ein VPN

On-Demand-Inhalte

Releasegruppen veröffentlichen TV-Sendungen und Filme vor dem offiziellen Starttermin. Die Struktur der Medienbranche bietet wegen der großen Anzahl verschiedener Organisationen und Personen, die am Produktionsprozess beteiligt sind, eine Reihe von Gelegenheiten. Zu den gängigen Methoden für die Videobeschaffung gehören:

- Angriffe auf Rechenzentren, bei denen Nutzeranmeldedaten oder Videoinhalte gestohlen werden
- Diebstahl von Nutzer-IDs, mit denen auf Videoinhalte über verschiedene Produktionssysteme zugegriffen werden kann
- Aufzeichnungen physischer Assets (heute weniger verbreitet) für das Sharing und die Verbreitung
- Hacks verschiedener Produktionssysteme, um direkten Zugriff auf Videos 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?

Piraten nutzen jeden möglichen Kanal und jede technische Innovation, um ihre Inhalte zu verbreiten, darunter:

- eigens entwickelte IP-Set-Top-Boxen, die auf vorprogrammierte TV-Streams zugreifen
- Software, die auf Streaminggeräten und PCs ausgeführt wird und die Verbreitung gestohlener Inhalte ermöglicht, z. B. Kodi-Add-ons
- Anwendungen, die per Sideloading auf beliebten legalen Streaminggeräten installiert werden
- Websites und Social-Media-Services, die nutzergenerierte Inhalte hosten, wie z. B. YouTube
- Websites, die raubkopierte Inhalte über Links streamen, die über Suchdienste oder soziale Medien gefunden 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 und ihres Altruismus eher zu Asset-Sharing-Modellen (z. B. Cyberlocker und Torrent-Sites) tendieren. Finanziell motivierte Site-Betreiber profitieren hingegen eher von einer Strategie mit illegalen Streaminggeräten und anderen Streamingmodellen, die legale Services nachahmen und mehrere Umsatzmodelle unterstützen.

Die Nachfrage

Es gibt viele Gründe, warum Menschen Piraten-Websites aufsuchen. Darunter finden sich finanzielle Begründungen, Ignoranz der weiterführenden Folgen und die grundlegende Fähigkeit, ohne irgendwelche Beschränkungen auf Inhalte zuzugreifen. VFT Solutions Inc. stellt im Bericht 2019 über Betrachter raubkopierter Inhalte viele verschiedene Profile vor, die hier zusammengefasst sind:

- **Der „Content-Anarchist“** glaubt an das Recht auf öffentlichen und ungehinderten Zugriff auf Online-Inhalte. Seiner Meinung nach ist jede Gebühr für Inhalte zu hoch und er meint nicht, dass Piraterie unmoralisch oder illegal sei.
- **Die „Robin Hoods“** sind weniger extrem in ihren Ansichten und offen für alternative Angebote. Dieses Profil nutzt keine Livestreaming-Services, sondern wirkt an der Verbreitung von gemeinsam genutzten Torrent-Dateien mit.
- **Der „Nutzenmaximierer“** rechtfertigt seine Handlungen damit, dass der weitverbreitete Konsum von Inhalten den Schaden für Rechteinhaber wettmacht, da die meisten Inhalte von flüchtigem Wert seien.
- **Der „faule Pirat“** ist sich oft nicht bewusst, dass Piraterie illegal ist, oder gibt das zumindest vor. Er wird durch Kosteneinsparungen, die große Verfügbarkeit sowie den einfachen Zugriff beeinflusst.

VFT geht davon aus, dass der „faule Pirat“ und der „Nutzenmaximierer“ ungefähr 70 % der gesamten Community ausmachen. Dementsprechend sollten Initiativen, die Nutzer informieren, von legitimen Services überzeugen oder für illegal bezogene Inhalte bestrafen, den größten Nutzen haben.

Können wir Piraterie aufhalten?

Die Antwort auf diese Frage lautet leider: nicht ganz. Die Erfahrung lehrt uns, dass es immer Piraten geben wird, die Inhalte missbräuchlich nutzen möchten – aus altruistischen oder kommerziellen Gründen. Doch es gibt einen Lichtblick. Wenn wir das Problem strategisch über die Wertschöpfungskette hinweg angehen, lässt es sich minimieren. Das heißt, dass eine verbesserte Zusammenarbeit aller Branchenbereiche – auf den unten genannten strategischen Feldern – eine langfristige Wirkung hat.

Daten

Eine offensichtliche Notwendigkeit ist eine Standardmethodik, anhand derer sich das Ausmaß und die Folgen der Piraterie weltweit bestimmen lassen. Die Verwendung unterschiedlicher Methoden und Techniken lässt keine kontinuierliche oder kontextbezogene Analyse zu und führt zu Verwirrung bei der Priorisierung von Aktivitäten oder beim Verständnis der Rendite von Anti-Piraterie-Initiativen. Die mangelnde Standardisierung könnte durch Branchenverbände wie die Alliance for Creativity and Entertainment (ACE) behoben werden, die eine Führungsrolle bei der Datenerfassung übernehmen.

Schulungen

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. Initiativen zur Aufklärung der Öffentlichkeit sollten die Menschen weiterhin daran erinnern, dass Piraterie ein Verbrechen ist und einen echten Einfluss auf die Lebensgrundlage der Geschädigten hat.

Rechtliche und behördliche Maßnahmen

Es gibt mehrere ausgezeichnete Initiativen von Branchenverbänden oder staatliche Initiativen wie FAPAV in Italien, die Videopiraten verfolgen und die rechtlichen Schlupflöcher auf der ganzen Welt zu schließen versuchen. Diese Bemühungen erfordern ein hohes Maß an Koordination sowie Zugang zu relevanten Daten.

Technische und betriebliche Maßnahmen

Die Zeit, in der Inhalte ungeschützt bleiben, ist längst vorbei. In der Praxis bedeutet dies jedoch, dass eine strategische Überprüfung der Betriebsabläufe und die Identifizierung schwacher Glieder in der technischen Wertschöpfungskette von der Produktion bis zur Verbreitung erfolgen muss und geeignete Maßnahmen zu ergreifen sind. Wir bezeichnen das als die 360°-Haltung.

Wenn wir das Problem strategisch über die Wertschöpfungskette hinweg angehen, lässt es sich minimieren.

Die 360°-Haltung

Nachdem wir uns die Mittel angesehen haben, mit denen Piratengruppen sich Videos beschaffen und danach verteilen, haben wir ein Framework auf der Grundlage von drei Kernprinzipien aufgebaut: Schützen, Erkennen und Durchsetzen. Mithilfe dieses Frameworks können Unternehmen die Bedrohungslandschaft basierend auf ihrer Rolle in der Branche strategisch überprüfen und relevante betriebliche und technische Initiativen implementieren, um die Auswirkungen zu minimieren.

Schützen

Schutz vor Credential Stuffing

Wie bereits erwähnt, ist Credential Stuffing ein beliebter Angriffsvektor, der von Piraten verwendet wird, um Zuschauerdaten zu erhalten. Dazu verwenden sie in der Regel automatisierte Bots. Hier unsere wichtigsten Empfehlungen:

- Programmieren Sie Anmeldeseiten/APIs mit OWASP. Schreiben Sie unter Einhaltung der OWASP-Best-Practices sicheren Code und führen Sie regelmäßig 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 Lösung zur Bot-Verwaltung wie Bot Manager Premier von Akamai, die Sie dabei unterstützt, ausgeklügelte Angriffe auf Anmeldedaten durch Überprüfung des Nutzerverhaltens und der Gerätetelemetrie zu verhindern.

Schutz vor Diebstahl aus Systemen

Diebstahl aus internen Produktionssystemen, digitalen Speichern oder der öffentlichen Cloud ist eine wichtige Quelle für raubkopierte Materialien. Der Diebstahl von Video-Assets lässt sich grob in folgende Kategorien aufteilen:

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

Unternehmen können verschiedene Technologien einsetzen, um das Risiko zu minimieren. Im Wesentlichen basieren sie auf dem Konzept von Zero Trust, einem Framework, das Unternehmen zur Transformation des Zugriffs auf Technologie nutzen. Die Kernkomponenten des Frameworks umfassen: sicheren Zugriff auf Ressourcen (unabhängig von Standort oder Hostmodell), die Durchsetzung einer 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 Nutzer und Geräte Zugriff auf Anwendungen und Daten. Außerdem werden Anwendungen und Nutzer vor hoch entwickelten Bedrohungen aus dem 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 zentrale Produktions- und Speichersysteme. Aufgrund der hohen Fluktuation bei den beteiligten Arbeitskräften stehen Medienunternehmen vor einmaligen Herausforderungen bei Bereitstellung und Entzug von Systemzugriff – manchmal von einem Tag auf den anderen. Mithilfe von Services wie Enterprise Application Access von Akamai können Berechtigungen für bestimmte Anwendungen schnell basierend auf dem Identitäts- und Sicherheitskontext des Nutzers und des Geräts erteilt werden, ohne Nutzern Zugriff auf das Unternehmensnetzwerk zu gewähren, aus dem Videos extrahiert werden könnten.

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.

Aufgrund der hohen Fluktuation bei den beteiligten Arbeitskräften stehen Medienunternehmen vor einmaligen Herausforderungen bei Bereitstellung und Entzug von Systemzugriff – manchmal von einem Tag auf den anderen.

Schutz vor Geo- und IP-Rechtsverletzungen: Piraten verwenden oft VPN-Technologien, um das Ursprungsland und die IP-Adresse nach der erfolgreichen Erfassung legitimer Abonnentendetails zu maskieren und den Stream weiterzuleiten. Proxy-Erkennungstechnologie wie die Akamai Enhanced Proxy Detection blockiert auf intelligente Weise Anfragen, die mit anonymen Proxys oder VPN-Services in Verbindung stehen, direkt an der Edge und verhindert so derartige Anwendungsfälle.

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. DRM bezieht sich auf die Tools, Standards und Systeme, die zur Beschränkung geschützter 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, bei welcher 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 – auf jeden Fall gegen nicht professionelle Piraten. Die Keys werden aber in der Regel von HTTP-Servern bereitgestellt und können kopiert und weitergegeben werden, sodass sie oft nicht ausreichen, um wertvollere Inhalte zu schützen.

Zur Verstärkung der Verschlüsselung verarbeiten fortschrittlichere DRM-Technologien 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 verwenden Geschäftsregeln, die definieren, wann und wie Schlüssel auf den verschiedenen Geräten verwendet werden können. Hierbei werden Kriterien wie Standort oder zeitbasierte Regeln überprüft.

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 Verschlüsselung nahezu in Echtzeit implementieren können.

Erkennen

Wie bei jeder Art von Diebstahl ist der Erfolg von Schutzmaßnahmen nie garantiert. Deshalb ist die Erkennung jeder 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. Die Originalmedien müssen in keiner Weise geändert werden, was einen Vorteil darstellt – ein Fingerabdruck kann jedoch nicht zwischen verschiedenen Kopien desselben Titels unterscheiden, d. h., welche Kopie eines Videos in der ersten Instanz weitergegeben wurde.

Watermarking

Diese Methode kann die Piraterie zwar nicht verhindern, mit ihr können Serviceanbieter jedoch Videodiebstahl erkennen, die Beteiligten identifizieren und dann dagegen vorgehen. Beim Video-Watermarking wird ein Muster von nicht erkennbaren und nicht entfernbaren „Bits" in eine Videodatei eingefügt. Indem diese Daten mit der Identität des Zuschauers verbunden werden, können Piraten verfolgt werden, die Inhalte entschlüsseln, kopieren und illegal verbreiten. Derzeit werden drei Hauptmethoden für Video-Watermarking verwendet:

- **Bitstream-Modifizierung.** Hierbei werden ausgewählte Bereiche eines Bildes modifiziert, 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.
- **Clientseitiges Watermarking.** Diese Methode funktioniert gut für die schnelle Watermark-Extraktion und kann auf älteren Plattformen wie Set-Top-Boxen implementiert werden. Hierbei wird über den Videostream auf dem Clientgerät ein grafisches Overlay gelegt, das sichtbar oder unsichtbar gemacht werden kann. Da das Wasserzeichen erst angewendet wird, wenn es das Client-Gerät erreicht, muss der Videostream zusätzlich geschützt werden. Clientseitige Technologien erfordern auch eine SDK-Bereitstellung, die in OTT-Umgebungen komplex sein kann.
- **Watermarking mit A/B-Variante.** Diese Methode zielt auf den OTT-Sektor ab. Hierbei werden zwei identische Videostreams erstellt, mit Wasserzeichen versehen und daraufhin clientseitig oder über CDN-Edge-Verarbeitung zusammengesetzt oder 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 Watermark-Extraktion erfordern, nicht geeignet.

Ein wichtiges Element jeder Watermarking-Strategie ist eine geeignete Überwachung, damit Durchsetzungstechniken gegen Piraten eingesetzt werden können. Es gibt Managed Services für die Überwachung, oder es kann Rat für die Entwicklung interner Funktionen eingeholt werden. Akamai arbeitet mit allen 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 Form der Erkennung ist die Echtzeitprüfung der Bereitstellungsprotokolle. In diesem Szenario wird durch gründliche Protokolluntersuchung eine Echtzeitübersicht betrügerischer Aktivitäten bereitgestellt – basierend auf autorisierten und nicht autorisierten IP-Adressen. Der Vorteil dieser Lösungen, wie z. B. Stream Protector von Akamai, ist die Fähigkeit, die Funktion je nach Situation ein- und auszuschalten. Dies ist ideal für den Schutz zeitlich begrenzter Rechte, z. B. bei Sportinhalten.

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-Events, dann sollten Sie dem Bereitsteller des illegalen Streams sofort den Zugriff entziehen. Hierzu gibt es verschiedene Methoden. Sie können sich zum Beispiel mit Ihrem Distributionsserviceanbieter kurzschließen, relevante Details austauschen und Streamingaktivitäten von der entsprechenden IP-Adresse blockieren. Dies kann jedoch einige Zeit in Anspruch nehmen. 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.

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

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

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 hat die Branche relativ schleppend reagiert. 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.

In diesem Whitepaper wurden verschiedene unmittelbare Anforderungen beschrieben, die für den Kampf der Branche gegen Piraterie essenziell sind. Dazu gehören einheitliche Daten über Piraterie, eine verbesserte und kontinuierliche Bildung der Öffentlichkeit, eine bessere Zusammenarbeit in der gesamten Branche und schließlich ein Vorangehen der Rechteinhaber aus allen Genres, um die Handhabung und Verteilung von Rechten zu einem unumgänglichen Thema zu machen.

Die gute Nachricht ist, dass viele dieser Punkte bereits umgesetzt werden. Die Forschung zu diesem Thema erhält immer mehr Aufmerksamkeit, es werden strengere Gesetze erlassen und Anbieter kombinieren Kompetenzen, um deren Potenzial zu maximieren. 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 MPAA), 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.

QUELLENANGABEN

Asia Video Industry Association. The Asia Video Industry Report. 2019.

Bevir. Cost of online piracy to hit $52bn. 2017. Abgerufen unter https://www.ibc.org/publish/cost-of-online-piracy-to-hit52bn/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

Enigmax. 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. Almost 5 million Britons use pirated TV streaming services. 2017. Abgerufen unter https://yougov.co.uk/topics/politics/articles-reports/2017/04/20/almost-five-million-britons-use-illegal-tv-streami

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. Ibosiola, 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

---

Akamai *Experience the Edge*

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, im Blog blogs.akamai.com oder auf Twitter unter @Akamai. Unsere globalen Standorte finden Sie unter www.akamai.com/locations. Veröffentlicht: Juli 2020.