LEITFADEN

Schutz für Videoanbieter –
Vom Unternehmen über die Inhalte bis hin zu den Zuschauern

Akamai

> *Sie sind drin. In der Kolonie. Hier drin. Sie sind drin. Sie sind drin!“*
>
> *– Bill Paxton als Private Hudson in „Aliens“ (1986)*

Handlungspunkt 1: Angriffe auf Unternehmen

Bei der Videoproduktion dreht sich alles um Zusammenarbeit. Mit dem Übergang zu dateibasierten Workflows in der Branche hat sich die Anzahl der Endgeräte erhöht, die auf eine Ressource zugreifen oder damit in Verbindung stehen. Folglich ist auch die Anzahl der möglichen Schwachpunkte bei Ihrer Sicherheitsabwehr angestiegen.

Nehmen Sie als Beispiel Freiberufler und Postproduktionsfirmen. Sie sehen sich in der Regel nicht als Angriffsziele. Selbst wenn sie sich dessen bewusst sind, verfügen sie möglicherweise nicht über die nötigen Ressourcen oder Fachkenntnisse, um angemessene Sicherheitsmaßnahmen zu gewährleisten. Dadurch werden diese Unternehmen zu idealen Zielen.

Der allseits bekannte *Orange Is the New Black*-Hack aus dem Jahr 2018 beruhte beispielsweise darauf, dass finanziell motivierte Angreifer eine Postproduktionsfirma kompromittieren konnten, die an der neuen Staffel der erfolgreichen Netflix-Show arbeitete. Sie stahlen die Mezzanine-Dateien und verlangten ein Lösegeld dafür.[1]

Bei einem kürzlich in den USA hinter verschlossenen Türen angebotenen Seminar mit dem Titel *Cybersecurity for Broadcasters*, an dem mehr als zwei Dutzend Unternehmen teilnahmen, bezogen sich die meisten Anliegen auf den Schutz von Remotezugriff und die Anbietersicherheit.

Die folgenden beiden Vorgehensweisen sind dabei sehr nützlich:

1. Implementieren Sie eine Strategie mit geringsten Zugriffsrechten durch Einsatz eines Zero-Trust-Netzwerkzugriffstools für Mitarbeiter und Auftragnehmer, die Zugriff auf wichtige Ressourcen benötigen.
2. Erkennen und blockieren Sie schädlichen Traffic innerhalb des Netzwerks über ein sicheres Web-Gateway (SWG).

Diese Zero-Trust-Ansätze verringern die Wahrscheinlichkeit, dass ein Dieb in den Datentresor gelangen kann. Wenn dies trotzdem gelingt, steht aber nicht ohne Weiteres ein Fluchtwagen bereit.

> *Mein Vater war Gelegenheitsdieb. Er sagte: „Jeder stiehlt. So ist das eben. Auch ich stehle, mein Sohn. Aber ich lasse mich nicht erwischen.“*
>
> *– Christian Slater als Mr. Robot, „Mr. Robot“ (2015)*

Handlungspunkt 2: Angriffe auf Videoanbieter

Im Jahr 2013 wurde die TV-Serie „Hannibal", ein Psycho-Horror-Thriller, wegen „niedriger Zuschauerzahlen" eingestellt. Die Serie wurde jedoch in dem Jahr als die Nummer fünf unter den am meisten illegal heruntergeladenen Shows eingestuft. Produzentin Martha De Laurentiis gab an, dass der Hauptgrund für die Einstellung von „Hannibal" Piraterie war.[2]

Im Juni 2019 gab die Fernsehanstalt BeIN Media Group aus Katar die Entlassung von 300 Mitarbeitern aufgrund rückläufiger Einnahmen bekannt. Der Grund? BeIN behauptete, dass der Konkurrenz-Sender beoutQ illegale Kopien der Premium-Sportinhalte von BeIN nutzte.[3]

Medienpiraterie gibt es schon seit den Zeiten des Stummfilms. Der Übergang zum Streaming und die globale Distribution macht die Arbeit für Bösewichte heute noch einfacher und profitabler. Studien zu den Auswirkungen von Piraterie variieren drastisch, doch Analysten stellen immer wieder fest, dass Video-Piraterie jährlich mindestens 1 Milliarde USD Einnahmen für Angreifer in den USA[4] und dazu 1 Milliarde EUR in Europa ausmacht.[5]

Außerdem ist die Piraterie ein facettenreiches Ökosystem, in dem Amateure in sozialen Medien Inhalte für ihre Freunde streamen, „Informationsanarchisten" Premieren über Release-Gruppen rippen und teilen, finanziell motivierte Angreifer ausgeklügelte Videoservices bereitstellen und sogar Nationalstaaten Piraterie im Rahmen ihrer Informationskriegs-Kampagnen nutzen.

Dagegen anzugehen, ist äußerst schwierig. Wir bei Akamai arbeiten mit vielen der weltweit größten Produzenten und Distributoren von Videomedien zusammen, um unseren Ansatz „Schützen, Erkennen und Durchsetzen" zu entwickeln. Zusammenfassung:

Schützen: Verhindern, dass Inhalte und Anmeldedaten gestohlen werden

- Schutz vor Diebstahl von Videoproduktions- und Speichersystemen
- Schutz vor Diebstahl von Zuschauerdetails, um erneutes Streaming zu verhindern
- Schutz vor Geo- und Rechtsverletzungen
- Schutz vor Verstößen bei der Wiedergabe

Erkennen: Ermitteln, wer gestohlene Dateien verwendet

- Umfassende Protokollprüfung als Echtzeitüberblick über illegale Aktivitäten
- Proxy-Erkennung von Nutzern von VPN-Services
- Identifizierung und Nachverfolgung gestohlener Dateien durch Wasserzeichen

Durchsetzen: Piraten, die Ihr geistiges Eigentum nutzen, das Handwerk legen

- Token-Zugriffssperrung, um Streaming von schädlichen IP-Adressen zu verhindern
- Stream-Modifizierung, um illegale Streams durch alternativen Inhalt zu ersetzen
- Proxy-Blockierung, um den erkannten Nutzer an der Verwendung dieser Proxy-IP zu hindern

> *Unser ganzes Leben ist im Computer. Führerschein. Sozialversicherung. Kreditkarten. Krankengeschichte. Alle Daten an einem Ort. Sie warten förmlich darauf, dass jemand sie ausnutzt. Und wissen Sie was? Genau das ist mir passiert. Und eins ist sicher: Ihnen wird genau das Gleiche passieren."*
>
> *– Sandra Bullock als Angela, „Das Netz" (1995)*

Das Finale: Angriffe auf Zuschauer

Im Jahr 2019 wurde in den USA unter großem Erfolg ein wichtiger neuer Abo-Service eingeführt. Doch innerhalb von 24 Stunden beschwerten sich einige neue Kunden in den sozialen Medien, dass ihre Konten gesperrt wurden. In diesem Fall war die Ursache kein Datendiebstahl, sondern ein Credential-Stuffing-Angriff.

Wenn OTT-Services (Over-the-Top) feststellen, dass das Konto eines Zuschauers kompromittiert wurde, muss der zahlende Kunde sein Konto in vielen Fällen zurücksetzen, um weitere Diebstähle zu verhindern. Dadurch wird zwar das geistige Eigentum des Unternehmens geschützt, aber im Endeffekt ein schlechtes Kundenerlebnis geboten.

Viele dieser Angriffe erfolgen in Form von automatischem „Account Stuffing". Eine Abwehrmethode ist der Einsatz eines Bot-Verwaltungstools, sodass keine Notwendigkeit mehr besteht, Konten zu sperren und zurückzusetzen. Ein gutes Tool dieser Art erkennt, wann sich eine echte Person anmeldet, und blockiert Bots, die vorgeben, diese Person zu sein.

Identität ist dabei einer der Grundbausteine der OTT-Revolution, die ein großartiges Zuschauererlebnis sowie profitablere abonnementbasierte und werbegestützte Geschäftsmodelle ermöglichen. Daher ist der Schutz der Identität sehr wichtig.

Die Auflösung: Rückkehr des Helden

Videoproduzenten und Distributoren bemühen sich zwar um die Entwicklung eines sichereren Ökosystems, wissen aber gleichzeitig, dass Kriminelle selbst nach einem fehlgeschlagenen Angriff lediglich ihre Wunden lecken und unbeirrt die nächste Attacke vorbereiten.

Akamai ist ein wichtiger Partner für Videobereitstellung und Cloudsicherheit, der Sie als „Sidekick" effektiv unterstützen kann. Informieren Sie sich darüber, wie wir Ihr Unternehmen, Ihre Anwendungen und APIs schützen und Ihnen dabei helfen können, Piraterie in den Griff zu bekommen und zu bekämpfen. Erfahren Sie, mit welchen Mitteln unsere Bot-Managementlösungen den „Angriff der Klon-Krieger" abwehren.

Bis bald in der Fortsetzung!

QUELLENANGABEN

1) Netflix hacked, 10 new Orange Is the New Black episodes leaked
2) Did pirates kill 'Hannibal'? | The Hill
3) BeIN axes staff claiming profits hit by piracy
4) Sandvine White Paper – Video and Television Piracy: Ecosystem and Impact
5) EUIPO Reports: Nearly €1B in illegal 'IPTV' streaming in 2018; overall piracy down slightly

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: Juni 2020