The show must go on: How to protect media content

By Paul Beattie

18 Jun 2020

In the media industry, your content determines whether you live or die. It's your crown jewels. Worth protecting at all costs. And the current pandemic has only made the stakes higher. With cinemas closed, production paused and online operations increasing, security is more important than ever. As people get used to new ways of working (including handling sensitive data remotely) and media content, like films, are moved to online release, there are more endpoints for cybercriminals to exploit to get their hands on valuable content and critical data.

Image source: Pixabay via Pexels.

From film or TV production through to news reporting in all its forms, preventing piracy and keeping your content and intellectual property secure throughout development, delivery and consumption must be a fundamental part of your business. What do media organisations need to consider when putting together their security strategies? And how many of these strategies cover the new security challenges we've seen as a result of the pandemic?

The security stakes are high in the media world

Any media company questioning the need to prioritise security need only run through a few loss scenarios to understand why. Getting hold of a major broadcaster's high-profile media content and holding the organisation to ransom is a big-ticket for cybercriminals. Think of the consequences if certain sequences or the ending of the new James Bond film were stolen and duplicated onto the internet before release, or the effect of a breaking news story being hacked during transit and manipulated into fake news, undetected. What would happen if a major streaming provider suffered a data breach and lost personal and payment details?

What a pandemic can teach us about cybersecurity
Raymond Pompon 3 Apr 2020

The ramifications of security failures are huge – both in terms of reputation and financial costs.

> *It’s not just production and revenue losses that face a media company; a data breach could bring significant fines for non-compliance with the regulations of every territory where they have customers/users.*

So, for example, a US over the top player taking subscriptions from European consumers must be familiar and compliant with the complexities of GDPR and PCI PSS.

The media industry is intensely vulnerable

Security threats in the media industry come from all angles. The most ‘everyday’ threat vector is the sheer number of employees and third-party workers who have access to your valuable content. Every individual could be a potential a weak point in the chain, be that through an unintentional lapse in security procedures or malicious actions. And the scale of remote working we’ve seen recently as a result of the pandemic puts a strain on normal security processes, particularly as tech-savvy media employees source their own devices and systems to help them get their jobs done more efficiently. Add to this common threats, like phishing via email (on the increase due to Coronavirus), and the scale of the security challenge is significant, even in large organisations that have already made major investments in end-user device security.

Interestingly, the fact that media industry workers are so tech-savvy can frequently work against your security with people assuming a high level of knowledge makes them safe from attack. Also, a heavy reliance on Mac devices and innovative tech in the creative sphere doesn’t necessarily mix well with standard security measures.

#BizTrends2020: 6 cybersecurity trends to watch in 2020

Charl Ueckermann 15 Jan 2020

The widespread use of personal devices and the spread of shadow IT as individuals race ahead of official corporate IT, especially now, could further exacerbate these weaknesses. You can imagine how vulnerabilities could arise if you take a frontline journalist, for example, battling to get a story submitted any way they can - using whichever collaboration tool will work, rather than the official corporate one, potentially over an unsecured network.

Securing the future of media organisations

In response to this threat landscape, media organisations are turning increasingly to building a zero-trust environment as a way of protecting the corporate crown jewels. In a zero-trust environment, you assume the worst - that all application access intentions are malicious or undesirable. Instead of trying to protect all the borders and paths across your network, you create ring-fenced islands of applications and data that you can protect in a much more focused way.

ABOUT PAUL BEATTIE

Paul Beattie is responsible for the UK and European sales operation within BT's Global media and technology sector where he currently leads a dynamic team of business account directors. Working with an extensive network of highly qualified consultants and partners, this team provides global security, cloud and networking solutions for multi-national customers. In this age of permanent digital transformation, Paul and team focus on helping customers make the right choices to ensure that best business outcomes are achieved.

- The show must go on: How to protect media content - 18 Jun 2020

View my profile and articles...