Why annual penetration testing for the media industry must evolve

BY ANNA HAMMOND · MARCH 6, 2024 · LAST UPDATED ON MARCH 6, 2025

The media industry is a major target for cyberattacks. With the constant evolution of technology, cybercriminals are developing increasingly sophisticated methods to exploit vulnerabilities and compromise systems. Traditional security measures, such as annual penetration tests, are no longer sufficient to protect media organizations from these evolving threats. It's clear that security testing for media organizations must evolve.

In this article, we will explore the expanding threat landscape for media companies and discuss why annual penetration tests are no longer enough to ensure their cybersecurity. We'll also emphasize the advantages of continuous security testing for better vulnerability prevention.

The expanding threat landscape for media companies

As the online universe expands, evolves, and becomes more complex, media moguls are finding themselves in the crosshairs of cyber crooks. Their treasure trove of valuable content, user data, and sensitive information makes them an attractive target for malicious actors.

Correspondingly, cyber attacks on media establishments can garner significant public attention. A poignant example of a breach attempt unfolded in February of 2023, targeting Virgin Media TV. This resulted in temporary disruptions to programming, but the company quickly implemented mitigation measures to address the issue.

Some of the top cyber risks threatening entertainment companies are industry-specific. Take, for instance, the allure of media platforms to hacktivists seeking to spread messages to broader audiences. Yet, many risks are shared with businesses across various industries. In December 2022, The Guardian, a well-known UK newspaper, experienced a ransomware attack. This incident caused operational disruptions and led to the compromise of personal data belonging to UK staff members.

The limitations of annual penetration testing

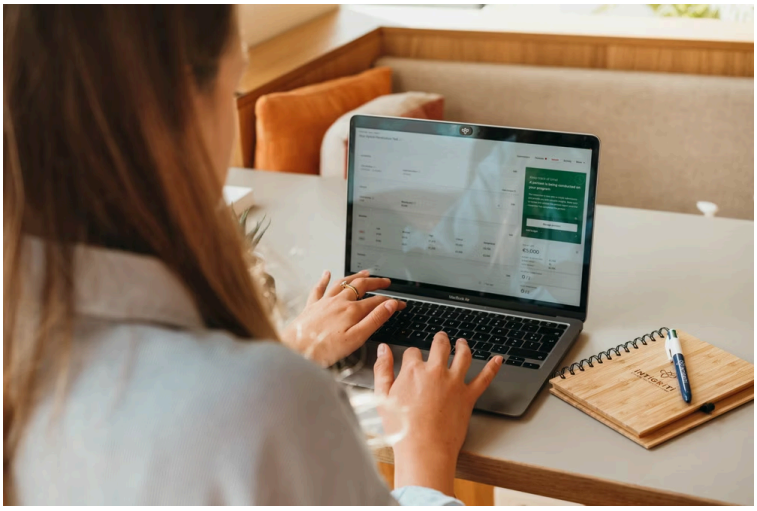
Although annual penetration tests can help safeguard media organizations against cyberattacks, they do have their drawbacks. For example, they only provide a snapshot of security at a single point in time. Therefore, they do not account for changes in the threat landscape or the organization's security posture over time. This can leave organizations open to attacks that exploit vulnerabilities that have developed since the last test was conducted.

Additionally, annual penetration tests can be costly and time-consuming, requiring significant resources to plan, execute, and analyze the results. This can be a burden for media organizations, especially ones with limited budgets and resources.

Finally, annual penetration tests may not provide sufficient coverage of all potential attack vectors. They typically focus on identifying vulnerabilities in external-facing systems and applications, but may not adequately address vulnerabilities emerging through operational processes and procedures. This can leave organizations exposed to a wide range of attacks that are not covered by the penetration test.

Continuous security testing for media organizations

Continuous security testing is crucial for identifying and addressing vulnerabilities before they can be exploited. This helps organizations stay strong and resilient against constantly changing threats.



Security testing professional hunting for vulnerabilities.

Let's dive into the details of how continuous security testing benefits media organizations. Continuous testing results in:

Proactive identification of vulnerabilities

One of the key advantages of continuous security testing is its ability to proactively identify security vulnerabilities in real time. By continuously monitoring and testing their systems, media organizations can detect and address vulnerabilities as soon as they emerge, preventing cybercriminals from exploiting them. This proactive approach significantly reduces the risk of data breaches, financial losses, and reputational damage.

Improved compliance with industry standards and regulations

Continuous security testing helps media organizations stay compliant with industry standards and regulations, many of which require regular security assessments and monitoring. Media companies can show they take security seriously by following strong security measures. This helps assure stakeholders, customers, and regulators that they are dedicated to keeping sensitive information safe and maintaining high security standards.

Reduced risk of data breaches and financial losses

Continuous security testing plays a vital role in reducing the risk of data breaches and the associated financial losses. By identifying vulnerabilities and addressing them promptly, media organizations can prevent unauthorized access to sensitive information, minimizing the likelihood of data breaches. This proactive approach not only protects customer data but also safeguards the organization from potential financial penalties, legal liabilities, and reputational damage resulting from data breaches.

Enhanced customer trust and reputation

By today's standards, customers expect organizations to prioritize the security of their personal information. Continuous security testing demonstrates a commitment to protecting customer data, enhancing customer trust, and building a strong reputation as a reliable and secure entity. This, in turn, fosters customer loyalty and retention, contributing to the long-term success of an organization.

Ability to quickly adapt to changing security threats

The cyber threat landscape is constantly evolving, with new threats emerging regularly. Continuous security testing enables media organizations to quickly adapt to these changing threats by identifying vulnerabilities and implementing appropriate countermeasures. This agility allows organizations to stay ahead of cybercriminals, minimizing the impact of attacks and ensuring uninterrupted operations.

How organizations can adapt pentesting to suit today's testing needs

To effectively combat the ever-changing threats, a proactive security approach is essential. This involves combining traditional pentesting with continuous testing methods, such as implementing a bug bounty program.

Check out Intigriti's on-demand webinar on how to optimize security testing budget.

Bug bounty programs and penetration tests share a common goal of identifying vulnerabilities that could be exploited by hackers. However, they differ in their approach. Pentests provide a snapshot of your security posture at a specific moment in time, accompanied by proof of attestation and an overview of vulnerabilities discovered within a defined timeframe. It's important to recognize that as you introduce new features or updates, your security posture may change. This is where bug bounty programs excel, serving as an ongoing initiative to continuously strengthen your security posture.

Another option for media organizations to evolve to is hybrid pentesting solutions, which combine the pay-for-impact approach of bug bounty programs with the dedicated resourcing strategy found with classic penetration testing.

Media organizations must evolve their testing strategy

The constantly-changing threat landscape poses significant challenges for media organizations, rendering annual penetration tests insufficient in safeguarding their assets and data. Continuous security testing

emerges as a crucial solution to effectively identify and mitigate vulnerabilities before they can be exploited by malicious actors.

By adopting continuous security testing, media organizations can gain proactive insights into their security posture, improve regulatory compliance, minimize the risk of costly data breaches and financial losses, enhance customer trust and reputation, and maintain agility in adapting to the ever-changing security landscape.

Don't let your media organization fall victim to preventable cyberattacks. Contact us today to learn more how Intigriti can help you stay ahead of the evolving threat landscape.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com