SPRING/SUMMER 2020 $25

The NOW WHAT? *Issue*

A new remote-work reality will mean long-term changes for how M&E gets business done. Welcome to Hollywood's new normal. *P. 15*

M AND E JOURNAL
Media & Entertainment
Strategies. Solutions.

published by
MESA
Media & Entertainment Services Alliance

Preparation and Learning From TPN Security Assessments … and COVID-19

Business continuity planning moves to forefront during pandemic

Photo by Dimitri Karastelev on Unsplash

By Chris Johnson, CEO, President, and Mathew Gilliat-Smith, EVP, Convergent Risks

Abstract: The M&E sector is united in improving digital security. There's a common pattern in the types of remediation needed and, in a rapidly changing environment, collaborating on intelligence is beneficial. Twenty percent of vendors already process content in the cloud but many are still trying to navigate security complexities. Here we explore the common themes, complexities in remediation and other info-sec topics related to corporate as well as content.

The M&E supply chain has never been more united in improving digital security. At the time of writing this article more than 500 vendors have, or are going through, the Trusted Partner Network (TPN) security assessment process, with hundreds more in the pipeline.

As a provider of TPN security assessments, the benefits are clear for us to see. Most facilities have some elements of Motion Picture Association (MPA) best practices that can be improved upon, and some have critical issues that fall below best practice which need to be immediately remediated. Importantly, no matter how minor or major the issue, security is improving across the board.

Convergent has been observing vendor-agnostic data since TPN launched, identifying trending types of remediation by geographic location. This rich data source allows us to report and respond to actionable intelligence targeting areas for future development. Collaborating on intelligence in a rapidly changing landscape can be extremely beneficial when raising awareness of the vulnerabilities to content as it moves through the creative and consumer process.

Common areas requiring remediation include: data IO, digital asset track-

Prior to **COVID-19,** only **20 percent** of new content reportedly was being **processed in the cloud.** This figure will **increase during the first half of 2020,** and by the **end of 2020** will have become established as a **business-as-usual** activity.

ing, dedicated CCTV VLAN, logging and event notification, and firewall implementation and configuration. Easily implemented items such as intrusion detection services (IDS), isolated internet on production workstations, are often lacking. In some cases, critical policies and business processes are missing entirely. A Convergent survey on penetration test reports recently found that 80 percent of vendors discovered findings previously unknown to them, with only 20 percent of vendors finding no issues. Furthermore, 40 percent of the findings were in the "critical" or "high" category requiring urgent remediation. Common findings were: security misconfiguration, SSL/TLS issues, components with known vulnerabilities and exposed management services. Sharing this information helps with better preparation.

An unprecedented event

One remediation item that has never been more relevant is business continuity planning (BCP). COVID-19 is proving a surreal situation and this current scenario feels more like we are living through a film script or industry experiment — only it is real, immediately impactive and extremely damaging.

Assessment and remediation, which earlier may have seemed a laborious task, are now seen by many as a very worthwhile effort when responding to COVID-19. An unprecedented event such as this will always make any response more difficult. In this case, the scale of transition to remote working and accelerated migration to application and cloud-based workflows has tested companies of all sizes. For many, this will be the first time BCP policy has been looked at since it was written. For others, such plans may not even exist. For those with a documented and tested BCP, remote working will have been a more swift and smoother transition.

With a large proportion of productions currently halted and limited new content to work with, areas such as localization and visual effects have been impacted especially hard. Add to this the significant risk of poorly managed configuration changes, increases in phishing attacks and malware, and the threat of unknown vulnerabilities sitting latent within our networks, and workflows will significantly increase the likelihood of future breaches.

To give some perspective, most of us have adopted and are rapidly adapting to new workflows that are likely to remain. Less travel means better corporate and social responsibility with less pollution and efficient cost-effective conversations via video call.

Move to the cloud quickly, securely

Prior to COVID-19, only 20 percent of new content reportedly was being processed in the cloud. This figure will increase during the first half of 2020, and by the end of 2020 will have become established as a business as usual activity.

Concerns over security in the cloud are changing in favor of achieving speed and efficiency. The cloud can be secured, but how you configure and monitor user interaction on a continual basis is critical. With so many moving parts involving third-party applications, navigating security is very challenging. While there is plenty of general guidance available, it is not always relevant or specific to media workflows.

Convergent's approach to protecting content is to make security available to the broadest possible audience, consistently and globally. Cloud and application security will be no different. We aim to be a leading advocate on the subject, providing assurance to content owners through industry-led best practice. While we await industry-led implementation, we will offer reviews based on the available standards and our industry knowledge, using a process of discovery, mapping and configuration testing.

Our three-step strategy includes scoping the relevant cloud architecture and applications to gain an in-depth understanding of the workflow, where content resides and likely areas of vulnerability. The next stage is mapping to best practices, highlighting areas for remediation. The third stage is conducting configuration reviews and penetration testing areas of concern and prior remediation. Significant investment has been made in training our media experienced workforce and integrating into our team cloud security architect professionals with in-depth knowledge of each of the cloud providers. ■

Chris Johnson *has been an M&E content security specialist since 2001, with a diverse range of experience and operational knowledge covering the music, gaming, studio and TV broadcast industries, including the production, post and digital distribution supply chains. chris@convergentrisks.com @ConvergentCEO*

Mathew Gilliat-Smith *has more than 25 years' experience in media, entertainment and information security, co-founding three new technology start-ups, and previously holding senior management positions in publicly listed media businesses. His passion revolves around new technology solutions, risk assessment and content security solutions for protecting against cyber-crime and piracy in TV, film and broadcast. mathew.gilliat-smith@convergentrisks.com @mathewgs*

convergent

GLOBAL EXPERTS IN THE IDENTIFICATION, ASSESSMENT & MITIGATION OF RISK

Cloud & Application Security Reviews
Mapping cloud and application security against industry best practices with regular configuration testing.

Pre-Assessment
Helping you prepare for TPN security assessments mapping your facility against best practice with support for remediation, engineering and management policies.

TPN Security Assessments
We are the leading provider of TPN security assessments with 450 completed assignments worldwide through our team of experienced assessors.

Penetration Testing
Through a targeted attack simulation, our team safely takes your business through real-world scenarios, with monthly vulnerability scanning and remediation advice.

PPI Privacy Compliance
Policy compliance services and verification that personal data is securely managed and protected across the supply chain.

Management Portal
Secure management portal and repository for managing work in progress for supply chains with full reporting and tiered communication.

Contact Us

For more information or general enquiries:

e: info@convergentrisks.com

w: www.convergentrisks.com

US Office: +1 (818) 452 9544

UK Office: +44 (0) 1276 415 725

www.linkedin.com/company/convergentrisks/

#convergentrisks

ConvergentRisks