M+E JOURNAL

Risks & Rewards

The opportunities before media and entertainment are unprecedented. So too are the threats.

OUR CHANGING INDUSTRY
The roadmap to media and entertainment's future is paved with innovation

LOCALIZATION
Content localization is a worldwide, need-it-now business. Here's how to keep pace

WORKFLOWS AND THE CLOUD
Cloud workflows are proving crucial for media productions today

SMART CONTENT
It's a data-driven content reality, and all the tools are there to realize success

21.02

RANSOMWARE: THE BOOGEYMAN THAT WASN'T

With proper incident response foresight there's no reason to become a victim of a ransomware attack

ABSTRACT: Hollywood knows best that when it comes to security: you can't put the genie back in the bottle. 2021 showed a post-vaccine Hollywood with greater access to viewers but also an increase in security horrors. At Richey May we are always innovating and thinking ahead to help our partners in M&E. Here we will help you get a better understanding of how ransomware has evolved and grown into the No. 1 issue in Hollywood.

By Jason S. Hamilton, Director, Cybersecurity Services, Richey May

MESA Platinum Member

Ransomware everywhere. We hear about it so frequently it has lost its novelty as a buzzword. It is such a commonly uttered term in fact, not unlike "the cloud," we should take a step back and define it to make sure we understand what it is at a fundamental level and see if we can pull back some of the boogeyman aura that has become associated with it. Once we're sure we know what it is, we can talk about how to prepare for it, detect its presence in our infrastructure, mitigate the damage, sanitize our systems, and recover from it with as little impact as possible.

WHAT IS RANSOMWARE?

Ransomware is a type of malware that infects a computer system and encrypts data files using an asymmetric encryption methodology, making critical data unusable. It contains a component which then informs the victim their data is being held hostage in this unusable format until a ransom is paid, and typically directs the user to transfer

funds to a crypto wallet in exchange for the private key needed to decrypt the compromised files. There is no guarantee the decryption key will be delivered, or that it will actually work when provided. There have been numerous cases where the ransom is paid and the victim receives nothing in return, leaving them to recover the data on their own, or accept the loss and move on. This begs the question: if an organization must lean on its own internal processes to recover the encrypted data anyway, then what was the point of paying the ransom or interacting with the perpetrator at all? This is an important consideration, so we'll circle back to this in a moment. First, let's talk about how we can proactively defend against a ransomware attack.

THE BEST DEFENSE: POLICIES, PROCEDURES, AND STANDARDS

Incident Response Procedures are a fundamental component of any security program. The first step in defending your network from a ransomware attack is to make sure you have a procedure for detecting and addressing potential threats. A suspicious event can be reported by a user, a Security Operations Center (SOC), or an alert from a monitoring system (e.g., files suddenly appear to be all written in wingdings, numerous files suddenly change ownership to a single user, or of course when the ransom demand is displayed on a workstation). Once a threat is detected, your IT team should first validate the threat, and then initiate the organization's Incident Response Procedure.

The Incident Response Procedure should include at least: defined roles and responsibilities of the Incident Response Team (IRT), data classification mapped to severity level, a decision tree to determine escalation levels and associated tasks, and a communication plan to understand whom to notify and when. It is also a good idea to create a separate procedure that is specific to ransomware, which includes how to validate the threat, mitigate the damage (i.e., re-imaging of infected endpoints), and recover as quickly as possible.

Network segmentation and logical segregation of data and business critical resources can also play a major role in proactively defending against a ransomware attack (and really, against any type of malware attack or active compromise). Fairly basic malware can easily locate mapped file shares and encrypt data located there as well. Locking down internetwork traffic with implicit deny policies can prevent malware from spreading, effectively isolating the threat and shortening the time to recover normal operations.

DO NOT PAY RANSOMS. Do take the time to ensure you have an incident response plan, a solid backup and restore procedure, and knowledgeable staff who are ready to execute those plans.

The key component of defense against a ransomware attack is to have a comprehensive backup strategy in place. Seems simple, right? It is simple, and yet somehow this fundamental procedure is ignored in the face of a real-time attack, decision-makers panic and ransoms are paid, perpetuating the cycle and benefitting only the attacker. Your organization's backup strategy should include: a list of business-critical resources such as servers, applications, and data warehouses; the frequency and methodology by which each resource is backed up; and the restoration procedure, organized in order of criticality.

The ransomware procedure mentioned above should reference backup strategy documentation and mandate that restoration processes be employed immediately following eradication of the threat from the network. The higher frequency with which backups are taken and the faster the restoration processing speed, the lower the impact to the organization. That's to say, TEST the restoration process frequently. Get better at it. Do it faster and with fewer errors and fewer redundant steps. The efficiency of your restoration process is directly proportional to productivity saved in the face of a ransomware attack.

That's it. That's really all there is to it. This is not theory; it is tested and proven in real world scenarios. Remember the Colonial Pipeline ransomware attack in May of 2021? Shortly after paying the nearly $5 million ransom, Colonial recovered their operations not by using the decryption tool provided by the hacker group who perpetrated the attack, but by restoring from their own backups. At the end of the day, paying the ransom was a pointless waste of time and money. Ransomware attacks should not be any more frightening than infection by any type of malware. With the right controls in place, cooler heads ultimately prevail. Do not pay ransoms. Do take the time to ensure you have an incident response plan, a solid backup and restore procedure, and knowledgeable staff who are ready to execute those plans. ⊞

Jason S. Hamilton *is the director of cybersecurity services for Richey May. He has more than 20 years of experience supporting and securing information systems and has held roles in many progressive cybersecurity positions supporting companies in data services, financial services, public-sector, and telecommunications.* jhamilton@richeymay.com *@RicheyMay*

Who Hollywood Calls When They're Hacked

We assess risk across your holistic tech stack and customize solutions to keep your assets safe.

Our deep industry knowledge means we are uniquely capable of anticipating your needs to achieve your strategic objectives. We are intimately familiar with IT operations and software development standards. Our broad spectrum of services means we can leverage the expertise of credentialed data privacy, cybersecurity and experts focused on business and IT risk, helping you thoroughly understand your risks and develop the appropriate mitigation efforts to reduce risk and maximize investments in people, process and technology improvements.

Roundtables for an opportunity to engage with your industry peers to exchange ideas and best practices in a facilitated, confidential, group discussion.

REGISTER HERE:
https://us02web.zoom.us/meeting/register/tZ0lf-uvqTspHdJLugzr44P-A6VZat4mDxhI

Contact us for a holistic tech stack that works across your entire enterprise.

Christian Calson
Business Development Director,
Media & Entertainment

Christian@richeymay.com
310.945.6284

info@richeymay.com

www.richeymay.com

Denver HQ | Charlotte | Los Angeles
Salt Lake City | Grand Cayman

RICHEY MAY Technology Solutions