FINAL PROJECT

USF Muma College of Business
UNIVERSITY of SOUTH FLORIDA

ISM6328.020 - Information Security & Risk Management

Professor

Dr. Marcus L. Green

- **Noor Ahamed Vempalle (U08615464)**

The MGM Resorts Cyberattack of 2023: Lessons in Cybersecurity Preparedness

1. Introduction

The *ALPHV/BlackCat* ransomware group set up a massive ransomware attack, in which MGM Resorts has become a victim in September 2023. This attack severely disrupted MGM's operations across its 30 properties, including the malfunctioning of casino floor systems, hotel reservation platforms, digital room keys, and customer service systems. Long wait times, unsuccessful transactions, and a lack of access to essential services were all experienced by customers, emphasizing the incident's significant operational and reputational effects.

The attack was an acute warning of the weaknesses in the cybersecurity defenses of large organizations and attracted international attention because of its complexity and severe consequences. This study looks at the attack's causes, preventability, future incident prevention strategies, and resilience-boosting policies. With the help of *97 Things Every Information Security Professional Should Know*, this case highlights how essential are proactive and flexible security measures.

2. Why the Incident Happened

Social engineering is a major weakness in human security procedures that the MGM Resorts cyberattack took advantage of. The attackers used voice phishing, or hacking,

to target an MGM employee. They acquired sensitive login credentials over the phone. The attackers used inadequate security measures to move laterally through the network, escalate privileges, and infect critical systems with ransomware after gaining access.

Contributing Factors

1. Inadequate Privacy Against Social Engineering: MGM's staff lacked the necessary skills to identify and prevent phishing attempts, even though social engineering is a known threat vector.

2. Weak Multi-Factor Authentication (MFA): The attackers reportedly discovered ways to get around MFA, perhaps by taking advantage of less secure MFA techniques like SMS-based codes.

3. Inadequate Network Segmentation: The attackers were able to move laterally within the network and reach systems that were essential to MGM's operations because of poor network segmentation.

4. Delayed Detection and Response: the attackers had sufficient time to escalate their access without setting off alarms, the attack exposes weaknesses in MGM's monitoring capabilities.

3. How the Incident Could Have Been Avoided

Preventing this attack would have required addressing vulnerabilities at multiple levels:

a.) Employee Awareness and Training:

- Staff members should receive regular training in phishing and hacking techniques.

- To evaluate staff members' capacity to identify and report social engineering attempts, simulated attacks were used.

b.) Advanced Multi-Factor Authentication (MFA):

- Making a transition to phishing-resistant MFA techniques like biometric authentication or hardware tokens (like YubiKeys).
- Weaker MFA techniques that are prone to interception, such as email-based or SMS-based authentication codes, should be reduced.

c.) Network Segmentation:

- Stringent segmentation is used to isolate important systems, making it difficult for attackers to access others even if one system is compromised.

d.) Tools for Early Detection

- Using behavior-based intrusion detection systems to spot suspicious activity, like unauthorized lateral movement or credential misuse.
- Recording and keeping an eye out for discrepancies in privileged account activity.

4. Preventative Measures for Future incidents

a.) Playbook for Incident Response

- A thorough incident response plan with explicit containment, suppression, and recovery procedures must be kept up to date and tested on a regular basis by organizations. Such a playbook ensures a quick reaction time in the event of an attack.

b.) Zero Trust Architecture

- By implementing a Zero Trust framework, the attack surface is significantly lowered.
- Authenticating and authorizing each request, regardless of its source, is one of the Zero Trust principles. Strictly limiting access rights to those required for a user's position.

c.) Recovery and Backup

- Keep regular offline backups of important data and systems to guarantee a solid recovery route in case of ransomware.
- Test backup systems frequently to ensure they are operating properly.

d.) Third-Party Risk Management:

- Regularly audit the security of partners and third-party vendors.
- Establish vendor-specific guidelines to make sure they follow the security requirements of the company.

5. Preventive Information Security Policies:

The following security measures could be placed in place by MGM Resorts to strengthen defenses and minimize potential threats:

a.) Social Engineering Policy: Create a mandatory anti-social engineering policy that outlines how staff members should respond to uncertain communications, particularly unauthorized emails or calls.

b.) Access Management Policy: Provide employees with the least privileged access, allowing them to access only the information required for their roles. Review and

remove unnecessary or unused access credentials on a regular basis.

c.) Vulnerability Management Policy: To resolve known vulnerabilities, software and systems must be patched frequently. To find and address vulnerabilities early on, performing routine penetration tests would help.

d.) Data Governance Policy: Clearly specify the levels of data classification and access limitations for sensitive data. Create encryption procedures for both in-transit and stationary data.

6. Important Takeaways from “97 Things Every Information Security Professional Should Know”:

i.) "The Human Element is Critical"

This attack serves as a reminder that people are frequently cybersecurity's weakest link. Just as crucial as technical protections are investments in strong social engineering defenses and employee awareness initiatives.

ii.) "Plan for Resilience"

It is impossible to overestimate the significance of having tested recovery plans. The difficulty MGM had resuming operations emphasizes the necessity of established, tried-and-true continuity plans to reduce operational disruptions.

iii.) "Zero Trust is the Future"

By limiting access to only authorized and verified users and preventing forward motion, a zero-trust architecture could have reduced the damage.

Conclusion

The MGM Resorts hack highlights how important it is for businesses to take a comprehensive approach to cybersecurity. MGM could have minimized the impact of the attack by addressing human vulnerabilities, putting in place more robust technical defenses, and making plans for resilience.

For other businesses, especially those in the hospitality sector, which are becoming more frequently targeted by cybercriminals because of the sensitive data they handle, this incident serves as a warning. In the face of changing threats, the lessons from MGM's experience emphasize the significance of proactive measures and ongoing improvement.

References

1. Abrams, R. (2023, September 12). MGM Resorts cyberattack disrupts casinos and hotels across the U.S. The New York Times. (https://www.nytimes.com)

2. ALPHV Ransomware Group. (2023). Details on the MGM Resorts ransomware attack. Bleeping Computer. (https://www.bleepingcomputer.com)

3. NIST. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

4. Limon, D., & Plaster, B. (2020). 97 things every information security professional should know: Collective wisdom from the experts. O'Reilly Media.

5. Wehling, C. (2023). What we learned from the MGM Resorts ransomware attack. Cybersecurity Dive. (https://www.cybersecuritydive.com)