Chris Bull

2/5/2025

CS-405

Module 5 Case Study

The case I will be discussing today is the MGM ransomware attack that happened on September 11, 2023 (<https://www.theverge.com/2023/9/11/23869020/mgm-resorts-hacked-casino-shut-down-las-vegas>). While not much has been publicly disclosed about this attack, it is known that the attack forced MGM computer systems down at various locations, including their casinos. At some points during the day, all the slot machines and ATMs were out of order within the casinos (Davis, 2023).

The attack was claimed to be performed by a group named ALPHV / BlackCat and was thought to be a ransomware attack (Davis, 2023). The group didn’t declare their motives, but the common motive behind a ransomware attack is for financial gain through extortion. The group likely wanted to hold MGM’s systems for ransom until they were paid through an anonymous bitcoin wallet. MGM was a target in particular because they deal with billions of dollars on a daily basis.

The immediate threats to MGM during this attack were the complete stalling of their company leading to lost revenue and the potential of data loss or data leaking. If the vulnerabilities that caused this attack go unresolved, it creates the potential for lawsuits against MGM for failing to protect customer data. There is also the possibility that the same form of attack can be used if it is not patched after the first attempt.

This specific attack was conducted with social engineering where a help desk employee’s data was found on LinkedIn and then impersonated through a call to MGM’s help desk. While the specifics of the attack past this are unknown, there are generally a few things a developer could implement to prevent this breach. One thing a developer could do is implement a robust MFA system for an extra layer of security on MGM employee accounts. This can help protect an account even when the attacker has the password. The developer could also limit each help desk employee’s access to only what they need. In doing this, an attacker may not be able to access sensitive portions of the system on a compromised help desk employee account.

When looking at this attack through the lens of Triple A security, there are many things that could be improved upon. For MGM to improve in **authentication**, it is important that each help desk employee has a strong username and password combination for gaining access to the system. This is also the phase where multi factor authentication should be set up. For MGM to improve in **authorization**, as previously mentioned, each help desk employee should only have access to the resources that they need for their job. Any extra permissions given to help desk employees adds to the risk if their account were to be compromised. Lastly, for MGM to improve in **accounting**, they should be recording usage logs on all accounts in the system. These usage logs might include things like “session duration, and data sent and received” (Mylonas, 2018).

While the previously mentioned Triple A security practices provide a great foundation for organizational security, it is encouraged that more layers are added. The process of stacking these layers on top of each other to create stronger overall security is known as defense in depth (Fortinet, 2024). Some other layers of security that could be added for better overall protection are network firewalls, anti-virus on endpoints, physical security. These all serve a different purpose but contribute to an overall more secure infrastructure.

**References**

Davis, W. (2023, September 11). *MGM “cybersecurity issue” shuts down slot machines and ATMs in Las Vegas casinos*. The Verge. https://www.theverge.com/2023/9/11/23869020/mgm-resorts-hacked-casino-shut-down-las-vegas

Fortinet. (2024). *What is Defense in Depth? Defined and Explained*. Fortinet. https://www.fortinet.com/resources/cyberglossary/defense-in-depth

Mylonas, L. (2018, November 27). *AAA Security: An Introduction to Authentication, Authorisation and Accounting*. Codebots. https://codebots.com/application-security/aaa-security-an-introduction-to-authentication-authorisation-accounting