MGM Data Breach

Introduction

MGM Resorts, which is one of the largest casino and hospitality operators in the world, suffered a significant cyberattack in September 2023. Even though comprehensive technical details weren't fully discovered, investigators concluded that a hacking group gained initial access via vishing (voiced phishing). The attackers targeted unsuspecting employees by impersonating IT staff or vendors over the phone to gain legitimate login credentials. In late 2023 it was discovered that the hacking group used MFA fatigue tactics which repeatedly prompted targeted employees for MFA approvals until one was mistakenly granted.

Once into their systems, they escalated their privileges to access critical systems. The attackers exfiltrated sensitive data and deployed ransomware that encrypted portions of MGM's IT infrastructure, leading to operational disruptions that lasted for nearly a week. During this time, their gusts faced a range of issues which included malfunctioning slot machines, ATMs, digital key cards, electronic payments systems, and online reservations. MGM had to switch to pen-and-paper methods to process transactions.

Risk Analysis:

Lack of DLP solutions: One of the primary risks contributing to the breach was the lack of DLP solutions. DLP solutions are a combination of tools, processes, and people that prevent and detect data breaches. Although the attackers gained unauthorized access using legitimate login credentials, utilizing DLP solutions could've help minimize the extent of stolen data the criminals obtained.

Vishing attack: The breach was initiated via a vishing (voice phishing) in which they impersonated IT staff to gain legitimate login credentials. These sort of attacks trick people into sharing sensitive information. MGM could have mitigated the likelihood of this attack succeeding by implementing anti-social engineering security awareness training to equip employees on the various tactics used in these attacks to recognize them.

MFA fatigue: This tactic was later found to be the method that the attackers used to gain unauthorized access. This type of social engineering attack involves sending a user too many MFA requests for them to eventually accept the request out of frustration. This too, could have been mitigated through security awareness training to help employees recognize this type of attack.

Applying NIST CSF to Mitigate Identified Risks

1. **Identify**
    - **a.** MGM would conduct a risk assessment to document its critical assets, the risks associated with those assets, and identify the potential ways that threat actors could gain unauthorized access to those key assets. MGM's critical assets in this breach was its data and customer information.
2. **Protect**
    - a. In this step, MGM should have implemented encryption protocols for its sensitive data, enforced strong access controls, and utilized authentication mechanics to safeguard its data from unauthorized access.
3. **Detect**
    - a. MGM should have implemented continuous monitoring solutions such as a SIEM tool to detect the repeated MFA requests that were made to lead to MFA fatigue.

Had this been implemented the attack would have been subverted and potentially led to an audit to improve their security posture.

4. **Respond**
    a. MGM should have developed an enhanced incident response plan as the attack led to operational disruptions that lasted for a week which caused for further loss in revenue. Implementing regular tabletop exercises so that their security team could have resulted in a timelier response to the incident and mitigated the consequences of the breach.
5. **Recover**
    a. Establishing a recovery plan that focuses on quick restoration of systems would be beneficial as this may have reduced length of time the operational disruptions lasted.

Conclusion

The data breach that MGM experienced was one that was caused by attackers implementing social engineering techniques such as vishing and MFA fatigue to gain unauthorized access into the company's systems. Retroactively analyzing this breach using the NIST CSF can help address areas of improvement such as data protection, authentication, and incident response. Ultimately, the resultant operational disruptions, reputational damage, and breach in the confidentiality of customer data may have been avoided. Since the methods the attackers use mainly involved exploiting human error, implementing controls such as security awareness training would have helped teach employees to identify and avoid such attacks. NIST CSF is completely free to access and use which would've been much more cost-effective than addressing the ramifications of the breach.

References

- Inszone Insurance. (2023). The cyberattack on MGM Resort explained. Retrieved from https://inszoneinsurance.com/blog/cyberattack-mgm-resort-explained
- BeyondTrust. (n.d.). MFA fatigue attack. Retrieved from https://www.beyondtrust.com/resources/glossary/mfa-fatigue-attack
- NextDLP. (n.d.). How to detect data exfiltration. Retrieved from https://www.nextdlp.com/resources/blog/how-to-detect-data-exfiltration