Armaan Kapoor

ECE455

Security Review #0

Part I

On Monday, September 11, 2023, MGM Resorts, an S&P 500® global gaming and entertainment company, issued a somewhat cryptic message:

> "MGM Resorts recently identified a cybersecurity issue affecting some of the Company's systems. Promptly after detecting the issue, we began an investigation with assistance from leading external cybersecurity experts. We also notified law enforcement and took immediate action to protect our systems and data, including shutting down certain systems. Our investigation is ongoing, and we are working diligently to determine the nature and scope of the matter."

In the wake of this announcement, customers of MGM's services took to Twitter and other social media platforms to voice their concerns. Reputable news outlets reported significant disruptions not only in hotel room key card readers but also in slot machines, ATM cash dispensers, and reservation services. Given the broad geographical scope of this cyberattack, affecting properties in multiple states, this review will focus on the most pressing issue: hotel room access.

MGM, as a renowned hospitality provider, has both a fiduciary and ethical duty to ensure the security of its guests. However, the cyberattack compromised this security by causing malfunctioning RFID key cards that locked guests out of their rooms and allowed unauthorized access to random rooms. A guest at the MGM Grand in Las Vegas reported walking into the wrong room due to malfunctioning digital keys, prompting staff to distribute physical keys as reported by BBC.

The likely aim of this cyberattack was to disrupt the databases and cloud services that MGM uses to manage their IoT (Internet of Things) infrastructure. Given that the attacker's intent was possibly to damage the company's reputation and manipulate its stock (which fell by 7.36% over the past month), it is probable that the attack originated externally. While specifics about MGM's network management are not publicly disclosed, it can be inferred that their operations engineers use a computerized check-in/out system that manipulates permissions associated with RFID/magnetic strip key cards issued to guests.

These key cards are passive components managed via CRUD (Create, Read, Update, Delete) operations in MGM's "secure" database. This database is likely connected to a centralized access control system that communicates with active door readers via secure protocols such as HTTPS or MQTT. While RFID and magnetic strip key cards are inherently vulnerable to physical exploits like cloning or skimming, these vulnerabilities are generally considered acceptable risks in the industry.

If an attacker gained privileged access to these databases through techniques like SQL injection or privilege escalation, they could potentially manipulate IoT devices like door readers. This would leave non-technical staff powerless to intervene and could necessitate a rollback to physical security measures, such as manual locks and keys, as was the case according to BBC reports.

MGM can now retrospectively analyze log messages, network traffic, and other digital footprints to identify the source of the compromise. The first step should be initial containment, both short-term and long-term. Short-term containment could involve isolating affected systems from the network to prevent further spread of the attack. Long-term containment might require more drastic measures, such as taking down servers or services for an extended period to conduct a thorough investigation. Once the root cause is identified, the next step is eradication, where the malicious elements are removed from the environment. This could involve patching vulnerabilities, strengthening firewall rules, or even rebuilding systems from scratch. Recovery may involve restoring and validating system functionality for business operations to resume. It's crucial to monitor the systems for signs of weaknesses that could be exploited again.

Due to the scope of the breach, customer outrage extended beyond the hospitality department to the BetMGM website and individual casinos. If payment or betting history was compromised due to the breach, the ethical implications would be severe. However, if MGM shut down these services as a precautionary measure, it would be considered a responsible action.

The outcry over the key card glitch is entirely reasonable, as safety is a matter of life and death. Policy in this area is already stringent, with compliance to standards like PCI DSS (Payment Card Industry Data Security Standard) and GDPR (General Data Protection Regulation) being mandatory. It remains to be seen what legal and regulatory consequences MGM may face for violating these policies. Lawmakers and cybersecurity experts should continue to monitor updates from MGM, which should also continue to report developments transparently.

Sources:
https://www.bbc.com/news/technology-66784894
https://www.google.com/finance/quote/MGM:NYSE?sa=X&ved=2ahUKEwiU6rz5wKWBAxW3lokEHU_BBHMQ3ecFegQIOxAh
https://www.fox5vegas.com/2023/09/11/computer-system-outage-disrupts-operations-mgm-resorts/
https://flipperzero.one/
https://www.oloid.ai/blog/how-do-rfid-cards-work/#:~:text=RFID%20cards%20work%20by%20emitting,physically%20touched%20by%20the%20scanner.