**MGM Resort Data Breach of 2019**

**Executive Summary:**

**What happened? -** On July 7th, 2019, MGM Resort’s databases were compromised by hackers. At the time of doing research on the incident, it is claimed that roughly around 200 million or more data records were stolen and possibly listed on the dark web for unethical profitable gains. Much of the data that was exposed from the data breach included personal information such as names, dates of birth, phone numbers, social security numbers, and addresses (Ikeda). Although MGM Resorts claim that no credit/debit card numbers or passwords were leaked, the affected users were still likely to become targeted for phishing attacks, identity theft, profiling, and password attacks on other online website accounts (State Of Nevada).

**How did it happen? -** It is claimed that the attackers were able to breach the databases and expose the records by either using social engineering and compromising user credentials or by searching for and exploiting vulnerabilities in their systems. It is also likely that the attackers had performed an SQL Injection attack to display the exposed information (State Of Nevada).

**Who was affected? -** The affected users in the incident included hotel employees, hotel guests, casino guests, celebrities, Database administrators, and IT officials. Some users like database administrators, technicians, IT help desk, and systems analysts had administrative privileges. Meanwhile, users like hotel management, hotel employees, and guests who had access to a guest computer were authorized as regular users with regular user privileges or guest users with most limited privileges (Morris).

**What can be done to protect the organization (#3) -** After the data breach, MGM Resort handled the incident in regard to protecting the company by training employees regularly on the best and simple cybersecurity practices that they can perform. They also reconstructed their policies on passwords and user privileges. This was done to enforce stronger passwords, change passwords more frequently, and have more control over the permissions for each user account. Some of the few things that would better assist the company in protecting the organization would be to protect the data, secure the WiFi points, and hire an ethical team of hackers to hack their systems. Protecting the data at the source can be done by using encryption to encrypt the data and only allowing authorized users with unencrypt keys to view the data. Creating backups of the data would also be included to help mitigate the risk of permanent data loss. MGM Resorts would also benefit from securing their WiFi access points. The current WiFi security of WPA2 is noted to be more secure than WEP network security and is recommended with the use of complex passwords for the WiFi access points. One of the last things that could help the organization is the assistance of a team of ethical hackers. Hiring a team of ethical hackers to search and exploit vulnerabilities in the systems would allow the organization to find the vulnerabilities in the systems and securely patch them before the attackers find and exploit them.

**What can be done to protect the customers (#4) -** After the incident happened, MGM reported the incident to law enforcement and also provided identity theft protection services to everyone who was affected by the data breach. This included services such as 12-month credit card and CyberScan monitoring and $1,000,000 reimbursement policies. However, providing these services is more of an act of response and not much so an act of prevention. The actions of protecting the customers’ data and training the employees on how to carefully handle the customers’ data would be very beneficial in preventing the data to be exposed and misused. Having the customers’ data encrypted and backed up properly would help to mitigate the risks of data breaches and permanent data loss and support data integrity. Meanwhile training the employees on how to properly handle customer data would promote better management of customer data.

**What can be done to fight against the growing threat of ransomware (#7) -**

As the rate of ransomware attacks increases, a few things can be done by MGM Resorts to be better prepared for ransomware attacks. The first practice would be to regularly create data backups and data recovery procedures. This would very likely help to mitigate data and financial loss. The reason being is that the company would very likely not have to pay a ransom if the data that is attacked and encrypted has an exact copy. Another addition to this that is common is to create 2nd backups and properly store them offsite. And lastly, the company would benefit from investing in robust anti-malware protection and including a ransomware response plan in the business continuity plan. This would better assist in real-time protection from ransomware attacks and responses in case a ransomware attack does happen.

Works Cited

Cimpanu, Catalin. “A hacker is selling details of 142 million MGM hotel guests on the dark web.” *ZDNet*, 13 July 2020, https://www.zdnet.com/article/a-hacker-is-selling-details-of-142-million-mgm-hotel-guests-on-the-dark-web/. Accessed 19 May 2022.

Ikeda, Scott. “New Details Indicate That Scope of the 2019 MGM Data Breach Is Much Bigger Than Expected.” *CPO Magazine*, 31 July 2020, https://www.cpomagazine.com/cyber-security/new-details-indicate-that-scope-of-the-2019-mgm-data-breach-is-much-bigger-than-expected/. Accessed 19 May 2022.

Morris, Chris. “MGM Resorts hack leaves 10.6 million guests affected. How to check if data breach impacted you.” *Fortune*, 20 February 2020, https://fortune.com/2020/02/20/mgm-resorts-hack-data-breach-10-6-million-guests/. Accessed 19 May 2022.

Parry, Wayne. “MGM still detangling last year's data breach.” *Las Vegas Review-Journal*, 8 June 2020, https://www.reviewjournal.com/business/casinos-gaming/mgm-still-detangling-last-years-data-breach-2048611/. Accessed 19 May 2022.

State Of Nevada. “MGM Resorts International Data Breach Litigation.” *Cohen Milstein*, 2 April 2021, https://www.cohenmilstein.com/sites/default/files/Amended%20Complaint%20-%20In%20re%20MGM%20Resorts%20Data%20Breach%20-%2004022021.pdf. Accessed 19 May 2022.