Case Study: 2023 MGM Cyber Attack From the Point of View of Social Engineering

Student Name: Liangshun Cheng

School of CyberSecurity, Old Dominion University

CYSE 201S: Cyber Security and the Social Sciences

Instructor: Diwakar Yalpi

Date:4/18/26

Introduction

The cybersecurity field often combines both technology and social sciences in order to protect data and people online. A specific issue that has been on the rise in recent years is the use of social engineering in Cyber attacks. Social Engineering attacks include manipulating the person behind the screen as opposed to manipulating technology or code. Using human behavior to create a vulnerability that attackers can use. An example of this can be clearly seen in the 2023 MGM cyber attack, where a type of social engineering known as vishing was used. Attacks like these are not something technology can solve easily; instead, the social sciences need to be applied, and ideas from fields like psychology and sociology will be needed in order to create countermeasures, so that people and organizations can better protect themselves against such attacks.

Research

The attack on MGM was carried out by a group known as Scattered Spider. They used a social engineering technique known as Vishing in order to trick the IT staff responsible for the Okta admin portal into creating an admin account for one of their members. This allowed the group into the system and allowed them to escalate their privileges and go where they should not be. This way of entry did not involve much technology at all, no network probing or searches until they were already inside. Instead, the group took advantage of Human psychology, and IT help desk training in order to trick an employee into handing them what they needed. There is also the fact that Vishing isn't the only form of social engineering to take advantage of people. Tactics like phishing and spear phishing done via email are all threats. Due to this fact, in order

to understand this breach, we need to look at the social sciences to understand what they did and not just the technology side of it. By understanding the human and social factors of this, a solution can be developed to prevent future attacks like this one.

Solutions

Solutions to attacks like the MGM cyber attack will primarily be focused on the human beind the screen instead of the system used. It is probably a good idea for regular online safety training in order to keep people informed and on their feet to expect attacks like this. Training like this should also take in the workplace societal practices into account. There is also societal norms outside the work place to take into account. Society in the modern age posts alot of information online, information hacking groups like Sacttered Spider used in this attack. Employees should be careful about what they post about themselves online or even on LinkedIn as information like this can give hackers a way to hack companies by understanding how workplace societies work. The implementation of a secure line or phone number recognition may also help prevent attacks like this. Essentially, training internal IT help desk workers to only pick up the phone if the number is known to be an employee, a system can also be put in place to filter out unknown numbers.

Barriers

Unfortunately, due to the nature of how social engineering attacks are, there is no one-size-fits-all solution. For computer systems, there are holes that can be patched with code or an update. However, when it comes to a social engineering attack like the one MGM faced, even proposed solutions will still not be 100% effective. Some people trust others more easily, making them especially vulnerable targets for these types of attacks. Help desk workers are trained by companies like MGM to help those on the other side of the phone, increasing the risk of a

vishing attack being possible. However, these obstacles can still be overcome. While the psychology of a person can't be rewritten, there are methods that can help. Having a structured response system and clear rules in place can make it so that even if the attacker has the trust of the person on the phone, they can't get access.

Reflection

As the field of cybersecurity grows, it will continue to incorporate social sciences into itself as it is needed. Technology can do many things, like patching system vulnerabilities and closing off software holes. However, the human behind the screen can't be fixed with a patch or system update. As such, you will need to understand the social sciences to create training and methods to combat social engineering. Fields like criminology, psychology, and sociology will also be needed to understand how cyber criminals thing and thus understand where they will attack so that you can better prepare yourself for said attacks.

Conclusion

In conclusion, the MGM cyber attack in 2023 was caused by a social engineering attack known as vishing, and in order to combat these types of attacks, we can't rely solely on technology. Instead, we need to look to the fields of social sciences in order to understand human behavior, criminal behavior and the behavior of wider and workplace societies in order to develop a solution that will prevent future attacks like this.

Works sited

Associated Press. (2023, September 13). *MGM Resorts cyberattack shuts down systems across Las Vegas Strip*. AP News. https://apnews.com/article/vegas-mgm-resorts-caesars-cyberattack-shutdown-a01b9a2606e58e702b8e872e979040cc

Brodkin, J. (2025, January 10). *News: Social engineering top cyber threat in 2025*. TechRepublic. https://www.techrepublic.com/article/news-social-engineering-top-cyber-threat-2025/

Cimpanu, C. (2023, September 14). *Okta: Caesars, MGM hacked in social engineering campaign*. TechTarget. https://www.techtarget.com/searchsecurity/news/366552775/Okta-Caesars-MGM-hacked-in-social-engineering-campaign

eBuilder Security. (2023, September 15). *Hack: How a 10-minute helpdesk call led to a multi-million-dollar breach*. eBuilder Security. https://ebuildersecurity.com/articles/hack-how-a-10-minute-helpdesk-call-led-to-a-multi-million-dollar-breach/

Ferreira, A., & Cruz, J. (2023). *The psychology of social engineering: Manipulation, scams, and human factors*. *Cybersecurity, 9*(1), Article tyac016. https://academic.oup.com/cybersecurity/article/9/1/tyac016/7000422)

Grimes, R. A. (n.d.). *How to avoid and prevent social engineering attacks*. TechTarget. https://www.techtarget.com/searchSecurity/tip/How-to-avoid-and-prevent-social-engineering-attacks

Grimes, R. A. (2023, March 22). *Social engineering: Definition, examples, and techniques*. CSO Online. https://www.csoonline.com/article/571993/social-engineering-definition-examples-and-techniques.html

U.S. Department of State. (2023). *Understanding the dangers of social engineering*. https://www.state.gov/understanding-the-dangers-of-social-engineering/