Texas Council Risk Management Fund

Caesars and MGM Ransomware Attack - How to Reduce the Risk of this Type of Incident

The attacks on Caesars and MGM Resorts show how even companies that you might expect to be fully locked down and protected from cybersecurity attacks are still vulnerable if the hacker uses the right attack method. In this case, it appears that publicly available information and a persuasive phone call were enough to give the hackers all they needed to get into the casino systems and created some very expensive havoc that will hurt both the resort chains and many of its guests.

A group known as Scattered Spider is believed to be responsible for the systems breach, and it reportedly used a ransomware-as-a-service operation. The group specializes in social engineering schemes, where attackers manipulate victims into performing certain actions by impersonating people or organizations the victim has a relationship with. The hackers are said to be especially good at "vishing," or gaining access to systems through a convincing phone call rather than phishing, which is done through an email. The hackers found an employee's information on LinkedIn and impersonated them in a call to the casino IT help desk to obtain credentials to access and infect the systems. The exact range of data stolen in the cyber-attack remains unclear, with the attackers only telling the media that they took six terabytes worth of information. Caesars disclosed that the attackers specifically accessed the "Caesar's Rewards" loyalty program database and agreed to not make it public in return for a ransom payment. The two major casinos now face a combined nine federal lawsuits since the attack.

Tips for preventing Ransomware.

1. Update systems with the latest security patches and software updates.
2. Mandate strong passwords and multi-factor authentication.
3. Regularly backup your data and store it offline in a secure environment.
4. Install and update robust anti-virus and anti-malware solutions that will detect intrusions.
5. Segment the network to limit malware movement in case of attack.
6. Conduct regular security training and simulated phishing attack exercises.
7. Constantly train all staff on safe online practices.

Tips for preventing Vishing.

1. Verify unexpected phone requests in ways that aren't connected to the incoming phone call. For example, use an official directory and another phone to call the company's main office and ask to speak with the caller who is making the request.
2. Be very suspicious of any caller who asks you to share login information over the phone.
3. If a caller asks you to provide account data or personally identifiable information, refuse to do so and report the contact to security.

4. Security won't phone you to request that you change logins, passwords, or network settings. Any caller who makes this type of request is probably a scammer. Refuse the request and notify security.

These tips don't only apply to our business environments, they can also be applied in our home lives. Regularly maintaining backups on home computers, making use of caller ID and being weary of unsolicited calls, and using complex lengthy passwords for system access are a cornerstone for good personal cyber health.

The TCRMF Cyber Risk Services Advisor is ready to schedule Cyber Risk Assessments and Incident Response Plan Tabletop Testing visits for members. Please contact Lee Cain by email at Lee.Cain@sedgwick.com or by phone at (512) 619-1437 to schedule services.