Caretcloud
Infinite Possibilities

Guide to Mitigate Cyber Threats &

Key business takeaways from MGM Data breach case

The Ultimate Guide

Caretcloud

Table Of Content.

Caretcloud

Everything you need to know about the MGM Data breach Case

A social engineering attack allowed the threat actor to burrow into the MGM environment and establish a foothold. Due to the common mistake of password reuse. attackers had usernames and passwords from previous data breaches. With additional information collected from a high-value user's LinkedIn profile, they hoped to dupe the helpdesk into resetting the user's multi-factor authentication (MFA). They were successful.

Based on available information, as it currently stands, threat actors also were observed creating persistence in MGM's network by configuring an entirely additional Identity Provider (IdP) in the Okta tenant using a feature called "inbound federation." The function is intended to allow the fast connection of different Okta tenants during mergers of companies.

It also appears that the attackers gained control not only of Okta but also of the Microsoft Azure cloud environment. This already jeopardized the applications managed by the IAM platform, but now all their cloud assets were also in danger.

MGM Resorts International

Global hospitality and entertainment company, with a portfolio of 29 hotel and resort properties, including iconic brands like Bellagio, MGM Grand and Mandalay Bay.

Allegedly, a criminal gang made up of U.S. and U.K.-based individuals that cybersecurity experts call Scattered Spider (aka Roasted 0ktapus, UNC3944 or Storm-0875) initiated a social engineering attack that led to the near shutdown of MGM Resorts International.

Caretcloud

Everything you need to know about the MGM Data breach Case

MGM team completely terminated the Okta platform and the threat actors' access initial access. HOWEVER, the damage had been done. The threat actors had already exfiltrated unknown terabytes of data and still had access to the cloud platform. It was time to make their presence known.

Using this RaaS service, Scattered Spider encrypted several hundred of their ESXi servers, which hosted thousands of VMs supporting hundreds of systems widely used in the hospitality industry. This caused cascading chaos. As the ESXi hosts became encrypted one after another, the applications running on them crashed … one after another … after another. Hotel room keys no longer worked. Dinner reservation systems were down. Point-of-sale systems were unable to take payments. Guests were unable to check in or out. Slot machines were completely unavailable. At this point, MGM was hemorrhaging money – and potentially its credibility.

Once the threat actors acquired their initial foothold, they could begin to escalate their privileges. They ultimately acquired the privileged access to the accounts running the IAM infrastructure. This allowed them significant access to the MGM network.
The full extent of what systems were compromised and what data was leaked is still unknown. Still, gaming industry analyst David Katz says that MGM Resorts is losing as much as $8.4 million in revenue every day until it fixes the problems caused by the ongoing cyberattack. There is still so much to this story that we won't know the full extent of the damage for quite some time.

Caretcloud

Mitigation Strategies to tackle data breaches

1. Contain Impact
Minimizing exposure of privileged accounts is vital in mitigating phishing attempts. IT administrators should use privileged access management (PAM) solutions, reducing the risk of compromise through attacks (including vishing). Organizations should also consider implementing zero standing privilege (ZSP) where applicable.

2. Improve MFA Control
Creating visibility into MFA device changes is essential. Implementing specific logs for customers to monitor in their security information and event management (SIEM) systems can help detect and respond to unusual authentication activities. Additionally, implementing a dual control feature can enhance security by requiring multiple authorizations for critical actions.
your Secure Zones.

Manage IdP administrator accounts in the same way database/domain admin accounts are managed (i.e., through privileged access controls such as rotating administrator passwords, monitoring/isolating admin sessions and enforcing dual access controls to access credentials).

Monitor trust changes, such as identity provider (IdP) modifications – it's essential for detecting suspicious activities. Organizations should consider implementing specific logs to track and analyze trust changes, providing valuable insights into potential security breaches.

Caretcloud

Mitigation Strategies to tackle data breaches

3. Protect Tier 0 Assets

Tier 0 assets must be protected, including signing keys and access to critical infrastructure. Implementing [endpoint privilege security] on federation servers can help safeguard signing keys from credential theft attempts. Furthermore, preventing unauthorized access to Tier 0 assets by limiting access to proxies along with dual controls is crucial.

4. Adopt IdP Best Practices

- **Implement MFA** controls before allowing users to change/alter their MFA factors (i.e., you must present a current MFA factor before altering one of your MFA factors enrolled).
- **Employ helpdesk verification controls** (i.e., the helpdesk may only reset a password once the user has verified their identity through a pre-existing enrolled MFA factor).
- **Always check a user's device enrollment/compliance** before allowing a user (especially an administrator) access to your IdP.
- **Identify secure zones in your network.** Understand network traffic to your IdP that does not meet your expectations. Limit actions that can be taken outside of your Secure Zones.
- **Manage IdP administrator accounts** in the same way database/domain admin accounts are managed (i.e., through privileged access controls such as rotating administrator passwords, monitoring/isolating admin sessions and enforcing dual access controls to access credentials).
- **Monitor trust changes such as identity provider (IdP) modifications –** it's essential for detecting suspicious activities. Organizations should consider implementing specific logs to track and analyze trust changes, providing valuable insights into potential security breaches.

Key Takeaways For Businesses.

Caretcloud

Key Takeaways For Businesses.

The Importance of Cybersecurity Layers: One of the key lessons from the MGM cyber attack is the critical importance of recognizing that relying on a single security measure is not enough to protect against sophisticated cyber threats. MGM's breach serves as a stark reminder of this fact. Businesses must adopt a comprehensive approach to cybersecurity by implementing multiple layers of defense. This can include firewalls, intrusion detection systems, endpoint security solutions, and robust employee training programs.

Regular security audits and updates: Cyber threats evolve rapidly, and businesses must stay proactive in identifying and addressing vulnerabilities. Regular security audits and system updates are essential to ensuring that a company's defense mechanisms are up-to-date and capable of fending off modern threats.

Incident Response Plan: MGM Resorts International faced significant chaos during the cyberattack, highlighting the need for a well-defined incident response plan. Businesses should have a clear protocol in place to respond swiftly and effectively in the event of a breach. This includes communication plans to keep stakeholders informed and minimize damage.

Caretcloud

Key Takeaways For Businesses.

Employee training and awareness: Human error is a significant factor in many cyber incidents. Employees may inadvertently click on phishing emails or use weak passwords, making it easier for attackers to gain access to systems. In the case of MGM, hackers appear to have employed social engineering by impersonating employees and making a fraudulent call to the service desk. Regular cybersecurity training and awareness programs can help employees recognize and respond to potential threats effectively.

Third-party risk management: Just weeks before the MGM breach, another Las Vegas casino fell victim to a serious ransomware incident. Caesars Entertainment says their customer data was accessed following an attack on an unnamed third-party IT vendor. Businesses must assess and manage the cybersecurity risks associated with their ecosystem of suppliers, partners, and service providers to mitigate external vulnerabilities.

Caretcloud

Caretcloud Offers Solutions.

01. Implement robust cyber security layers by implementing an Intrusion Detection and Prevention System.
02. Independent Cloud Security Assesment.
03. Cloud Security GAP Identification and Remediation.
04. Monitoring and Threat Detection by Building SOC and SIEM dashboards.
05. 24/7 Continuous Monitoring and Threats detection by managed SOC.