url: /lessons-from-MGM-attack

Title: CAUTION DISTURBING MATERIAL: Lessons from MGM

image: 9_19_client_data-breach.jpg

Image tag: data-breach

Disturbing. All cyberattacks are disturbing, but the recent MGM cyberattack should rattle you to the core.

Why?

Because it has so many disturbing elements, and every single one could happen to your organization. But let's look at the most disturbing facet of this attack: HOW it happened.

Did the attackers use complex code?

Nope.

Did the attackers use expensive digital tools?

Nope.

The HOW of attack boils down to the jarring fact that sometimes the weakest link in cybersecurity isn't the software or hardware. It's the HUMAN ELEMENT.

You've probably got a million questions right, but let's start by understanding the threat that took down MGM.

In the MGM breach, the culprits were the infamous Scattered Spider group and their associated BlackCat ransomware.

Their primary weapon? Social engineering.

Simply put, they manipulate individuals into giving away crucial information, often starting with something as simple as a phone call.

Steps to Protect Yourself and Your Organization

Okay, so this is scary stuff, but the good news is that you're not helpless and you're not alone. Here are some key steps you can take to safeguard yourself and your organization. First, let's talk about you:

- Be Skeptical: If you receive unsolicited communication asking for any form of personal or company data, be wary. Always double-check the authenticity of the source.
- Continuous Learning: Regularly educate yourself about the latest scams and tactics used by cybercriminals. Many organizations offer basic cybersecurity awareness training; take advantage of it.
- Protect Personal Data: Avoid sharing personal information, like your date of birth or home address, on public platforms. This data can be used by attackers in spear-phishing campaigns.

- Strong, Unique Passwords: Ensure your passwords are strong and varied across different platforms. Consider using a password manager.
- Regular Updates: Always update your devices and software. These updates often contain patches for known security vulnerabilities.
- Two-Factor Authentication: Wherever possible, activate two-factor authentication. This adds an extra layer of security, making it harder for attackers to gain unauthorized access.

So, those are steps you can take on a personal level, but about contributing to your organization's security if you're not a technical person?

- Be Aware Of Your Surroundings: Is there a general awareness in your organization about cyber threats? Are there regular training sessions or communication about this topic?
- Reporting What Doesn't Seem Right: If you spot a suspicious email or communication, is there a clear procedure to report it?
- Get A Second Check On Your Security From a Third-Party: Does your organization vet third-party vendors or partners for their cybersecurity measures? One weak link in the chain can compromise the whole system.
- Ask Questions: If you're unsure about something, ask. It's better to question something that looks off than to assume it's okay.

Final Thoughts

Every individual, technical or not, plays a pivotal role in cybersecurity. By staying informed, being cautious, and advocating for better security practices within your organization, you can contribute to a safer digital environment for everyone.

Remember, this may be a scary story, but you are empowered to create a happy ending.

Description Tag:

Every click counts! Learn how YOU can be the shield against major cyberattacks like MGM's. Be the change