timus

Could the MGM ransomware attack happen to you?

What happened: A hacker group specializing in social engineering applied a ransomware attack to MGM Resorts. By pretending to be an MGM employee, the hacker group was able to obtain credentials from the IT help desk, giving them broad access to MGM's network and making it possible to infect the system with ransomware. The truth is the MGM hack is not unique, and ransomware attacks happen to companies of all sizes and across all industries. Here are some eye-opening cybersecurity statistics.

$10 Trillion

Cyberattacks are expected to cost more than $10 Trillion in damages by 2025.

McKinsey estimates damages from cyberattacks will amount to more than $10 trillion annually by 2025 — a 300% increase from 2015.

Source: McKinsey & Company
https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

300% increase in cyberattack damages from 2015 to 2025

There are **three primary** openings for attacks.

Stolen Credentials

Phishing



Exploitation of Vulnerabilities

Source: Verizon
https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/

74% of breaches include a human element

74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of Stolen Credentials, or Social Engineering.

95% of attacks are financially motivated

95% of attacks are financially motivated, and 83% of the time it's done by an external actor.

24% of breaches are ransomware

Ransomware is the most common approach taken by attackers — 24% of all attacks include ransomware.

Source: Verizon
https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/

How can I protect myself against ransomware attacks?

Here are the two most important steps you can take to protect your organization.

1. Replace your VPN with a Zero Trust solution:

VPNs are subject to credential theft because they tend to give broad access to your network in one swift move. Adopt a Zero Trust Network Access solution like Timus to access data and apps remotely.

2. Augment your hardware-based firewall with an Adaptive Cloud Firewall:

Hardware firewalls were built for a time when data lived inside the walls of the office. Today, apps, data, and people are everywhere. Adaptive cloud firewall solutions like Timus protect company networks and data, no matter where the data lives.



Timus is the network security solution for the cloud era.

Timus helps companies orchestrate secure access while protecting the network against cyberattacks.

Timus combines secure, zero-trust network access with an intelligent cloud firewall that adapts in real time.

Get started in less than 30 minutes
timusnetworks.com