Security in the Live Event Industry

4 MIN READ

DEFENDING THE DIGITAL GATES

Protecting Your Live Event Organization From Cyber Attacks

The live-event industry has gone digital in a big way. From performing arts to sports and music, everything—from ticket sales to fan engagement—happens online. But here's the catch: that digital goldmine attracts more than just fans. Cybercriminals are lurking in the shadows, ready to pounce on weak spots in your systems. As an industry, we all need to band together to defend each other against bad actors. Here, we'll talk about five of the biggest cyber-security threats facing live-event organizations and how you can protect your organization from these digital villains.

CREDENTIAL STUFFING

The Bad Guys Love Your Passwords

Credential stuffing is a cyber attack where hackers use stolen login information from one breach to access accounts on other platforms. If you've ever reused passwords, you're not alone—and that's exactly what cybercriminals are banking on. Credential stuffing attacks are alarmingly prevalent, with Akamai reporting over 193 billion attacks in 2020 alone. According to F5 Labs, over 50% of all login attempts across various sectors are malicious, underscoring how widespread this threat is.

In preventing these threats, the strongest safeguard for your organization is Multi-Factor Authentication (MFA). This adds an extra layer of security, making it much harder for hackers to gain access with just a password. Microsoft's research shows that MFA blocks 99.9% of credential-based attacks. Additionally, educate your team and customers about the importance of unique, strong passwords. Offering password managers can simplify this process and encourage better practices. Lastly, employ behavior monitoring tools to detect and respond to unusual login activities, such as access attempts from unfamiliar locations or devices.

PHISHING AND SOCIAL ENGINEERING

Hackers With Charm

Phishing and social-engineering attacks trick individuals into sharing sensitive information or installing malware by pretending to be a trustworthy entity. The scale of phishing attacks has seen a dramatic rise, with the APWG reporting a 61% increase in such attacks from 2021 to 2022. Furthermore, Verizon’s Data Breach Investigations Report highlights that 74% of breaches involved human error, indicating that phishing and social engineering are significant drivers in the growing problem of security breaches.

Combating these threats begins with regular training for your staff. Educate them to recognize suspicious emails and links and to be cautious about sharing sensitive information. Investing in email filtering tools can help block phishing attempts before they reach your inbox. Using standards like DMARC, which is used to add an automated protective filter on incoming emails, can enhance your defenses against spoofed emails. Finally, implement anti-phishing tools that alert users if they encounter potentially harmful emails or links, providing an additional layer of protection.

RANSOMWARE

Cyber Kidnappers Holding Your Systems Hostage

Ransomware attacks lock you out of your own systems, demanding payment to regain access. The financial impact of these attacks is staggering, with Cybersecurity Ventures predicting a cost of $265 billion annually by 2031. In 2022, the average cost of a ransomware attack, excluding ransom payments, was $4.54 million, according to IBM.

To protect against ransomware, ensure that all your data is regularly backed up and stored offsite or in the cloud. In addition, many cloud storage providers offer disaster recovery packages that provide a second redundancy to ensure that you can recover your systems without succumbing to ransom demands. Keeping your software up to date with the latest patches is crucial, as updates often include fixes for vulnerabilities that ransomware can exploit. Additionally, investing in endpoint detection and response tools can help identify and mitigate ransomware threats before they spread.

BOT ATTACKS

The Ticket-Snatching Villains

Bots are used by digital opportunists to scoop up large numbers of tickets the moment they become available, often leaving real fans empty-handed and resulting in tickets resold at inflated prices. According to Imperva, 28% of all internet traffic consists of bad bots. The National Association of Ticket Brokers (NATB) estimates that bot attacks cost the live-event industry over $1 billion annually.

To defend against bot attacks, start by implementing CAPTCHA systems to differentiate between human users and bots. Tools like reCAPTCHA can help filter out automated traffic. Consider using a virtual queue system to manage ticket sales and slow down the purchase process, reducing the chances of bots grabbing all the tickets. Additionally, employing rate limiting can control how many requests a user can make within a certain timeframe, further mitigating the impact of bot attacks.

DATA BREACHES

Guarding Your Goldmine

Data breaches are not just a financial issue; they also damage your organization’s reputation and trustworthiness. In 2021, over 22 billion records were exposed in data breaches, as reported by Risk Based Security. The average cost of a data breach for the entertainment and media industry is $4.35 million, according to IBM.

To minimize the risk of data breaches, start by encrypting data both in transit and at rest. This ensures that even if hackers gain access to your systems, the stolen data remains unreadable. Implement strict access controls so that only authorized personnel can access sensitive information, and regularly audit these permissions. Conducting regular security audits and penetration testing can help you identify and address vulnerabilities before attackers exploit them.

WRAPPING IT UP

Cyberattacks in the live-event industry are a serious threat, but with proactive strategies, you can keep your operations secure and your audience happy. By addressing the risks of credential stuffing, phishing, ransomware, data breaches, and bot attacks with robust defenses—such as multi-factor authentication, encryption, employee training, and advanced bot protection—you can stay ahead of these digital threats. Protecting your digital gates ensures that your events run smoothly and your fans continue to enjoy the shows they love.