CANNABIS NEWS YOU CAN USE
CANNABIS RISK MANAGER

Cannabis Cybersecurity Threats: Protecting Your Business Data

The Growing Threat of Ransomware in the Cannabis Industry: Why Cannabis Firms Are at Risk

In recent years, ransomware attacks have spiked globally, and the cannabis industry is increasingly being seen as a prime target by hackers. Cybersecurity experts are warning cannabis businesses of the significant threats they face, particularly in light of high-profile breaches, such as the November attack on California-based cannabis producer Stiiizy. The attack, carried out by the Everest ransomware group, compromised the personal data of more than 422,000 clients and affected a software-as-a-service (SaaS) vendor serving Stiiizy.

Ben Taylor, executive director of the Virginia-based Cannabis Information Sharing & Analysis Organization, pointed out that in the past two years, he has tracked at least six ransomware incidents within the cannabis sector. These attacks, which involve encrypting or stealing data and demanding a ransom, have become alarmingly common. Ransomware can be financially devastating, with companies often forced to pay huge sums in Bitcoin or face the release of sensitive data on the Dark Web.

Understanding Ransomware Attacks and Their Impact on Cannabis Businesses

Ransomware is a form of cyberattack that locks a company out of its systems and demands a ransom for the release of the data. It has been a growing threat across industries, and the cannabis sector is no exception. Cannabis companies are increasingly vulnerable because they are in the process of rapidly scaling their operations and often lack the cybersecurity infrastructure of more established industries.

As ransomware attacks have skyrocketed globally, many cannabis executives have become more aware of the cyber threats facing their businesses. However, despite the growing threat, many cannabis companies still have gaps in their cybersecurity strategies.

Ransomware is a persistent issue across sectors, but the cannabis industry’s relatively young and evolving nature makes it especially vulnerable. As cannabis companies scale quickly to meet demand, they often fail to invest in proper digital security measures. Many businesses in the industry are more focused on operations, compliance, and product development than securing their digital infrastructure. This makes them ripe targets for hackers.

The Stiiizy Data Breach: A Wake-Up Call for the Cannabis Industry

The breach at Stiiizy, one of the largest cannabis producers in California, highlighted the gravity of cybersecurity risks facing the cannabis industry. In addition to compromising 422,000 clients’ personal data, the breach also infiltrated the back end of one of Stiiizy’s SaaS vendors.

While data breaches are not uncommon in many sectors, the cannabis industry's reliance on both physical and digital security systems makes it a particularly attractive target for cybercriminals. These kinds of breaches not only cause immediate financial damage but also long-term reputational harm. Stiiizy's breach underscores how a failure to protect consumer data can damage trust and credibility in the market.

Why Cannabis Companies Are Soft Targets for Hackers

David Wheeler, CIO of North American cannabis company TerrAscend, explains that the cannabis sector's rapid growth and often inadequate cybersecurity frameworks make it an appealing target for ransomware hackers. "The cannabis industry is young and fast-moving, and we're often upgrading the rocket while it's already in flight," Wheeler said. "Hackers know this and often target industries that are scaling quickly, assuming vulnerabilities exist due to growing pains."

Kay Yut Chen, Ph.D., a researcher in cybersecurity and ransomware, echoed Wheeler's sentiment. "Cannabis companies often focus on the core aspects of the business, like production and distribution. Cybersecurity doesn't always top the list of priorities," said Chen, a professor of Information Systems and Operations Management at the University of Texas at Arlington. As a result, cannabis firms may lack the expertise or resources to secure their data effectively.

Furthermore, cannabis businesses may face additional challenges when it comes to cybersecurity. According to Ed Rojas, founder of the Ransomware Defense Initiative, many cannabis firms are working with limited budgets and staff. As a result, Chief Information Security Officers (CISOs) in cannabis companies may have to compete for resources with other departments, such as IT, marketing, and sales. This often leads to cybersecurity being underfunded and deprioritized.

Essential Cybersecurity Measures Cannabis Businesses Should Implement to Safeguard Their Data

Despite these challenges, there are several proactive steps cannabis businesses can take to secure their data from cyberattacks. Experts agree that focusing on foundational cybersecurity controls is key to mitigating risks.

Vulnerability Scanning and Software Patch Management

Regular vulnerability scans can help identify weaknesses in a company's network and systems. Keeping software up to date with the latest patches can prevent hackers from exploiting known vulnerabilities.

Two-Factor Authentication (2FA)

Implementing 2FA is an easy and effective way to strengthen access controls. By requiring two forms of identification before granting access to sensitive systems or data, companies can add an extra layer of protection against unauthorized access.

Employee Training and Security Culture

A major avenue for cybercriminals to gain access to company data is through phishing attacks. Educating employees about the risks of phishing and providing regular cybersecurity training is essential. Taylor emphasized that creating a security-conscious culture within the organization can greatly reduce the likelihood of a successful cyberattack.

Endpoint Protection and Continuous Monitoring

Investing in endpoint protection and setting up continuous monitoring systems can help detect and mitigate cyber threats in real-time. This allows companies to respond quickly if an attack occurs.

Clear Incident Response Plan

Developing a robust incident response plan is critical. Employees should know exactly what to do in the event of a ransomware attack or any other cybersecurity incident. Regularly testing this plan through simulated exercises can help ensure a smooth response when real threats arise.

What to Do If Your Cannabis Business Falls Victim to Ransomware

Even with the best preventive measures, ransomware attacks can still happen. Experts advise against paying the ransom, as it only encourages cybercriminals to continue their attacks. Chen, who has extensively studied the consequences of ransomware attacks, suggests that businesses should follow the FBI's advice and avoid negotiating with hackers.

Instead, cannabis businesses should focus on strengthening their backup systems and ensuring they have multiple, secure copies of critical data. If an attack occurs, restoring data from backups is the best course of action.

However, some businesses may find themselves in a situation where the cost of downtime and lost business is too great to ignore. In such cases, negotiating a lower ransom fee may be an option, though it still carries significant risks.

Cybersecurity Must Be a Priority for Cannabis Companies

With the cannabis industry's rapid growth and its increased exposure to cyberattacks, it's crucial for companies to prioritize cybersecurity as part of their overall business strategy. By implementing foundational security controls, educating employees, and preparing for potential attacks, cannabis firms can protect themselves from the rising threat of ransomware and other cyber risks.

The time to act is now—before a breach puts your business, and your customers, at risk.

Email: info@cannabisriskmanager.com | Phone: +415-226-4060