Maestro Says Hoteliers Must be Diligent to Protect Against Ransomware

If hotel data is hosted in the PMS provider's cloud environment, backups will be automatically done and managed, and better secured against these threats

MARKHAM, ONTARIO, CANADA, January 26, 2022 /EINPresswire.com/ -- Maestro, the hospitality industry's leading provider of cloud or on-premises Web browser property-management systems for independent hotels, is warning operators about the seriousness and rising prevalence of ransomware attacks. If hotel data is not protected, properties could potentially lose access to their data overnight. Not only would this be inconvenient, but it would threaten operations and negatively impact business in a myriad of ways.

> A hotel's first defense against ransomware is preventing it from gaining access to the property's system."
>
> *Warren Dehan*

Ransomware is a category of malicious software designed to prevent users from accessing infected machines. Once infected, users find themselves unable to access their data and are prompted to pay a "ransom" to regain access to their files. While paying a hacker for access to your own computer is difficult to believe, impacted users are encouraged not to interact with the anonymous originator of the virus or provide payment. These activities will embolden hackers, enabling them to compromise further machines in the future and fail to guarantee your machines will remain safe from repeat hacks in the future.

More than 500 million ransomware attacks were estimated to have been attempted by hackers in the first nine months of 2021, making last year the most expensive for data security on record. The only way hotels can defend themselves against these incursions is by practicing good data stewardship by diligently recording backups — and by educating hotel staff about potential

vulnerabilities going forward.

Rather than play along with a hacker and hope they hold up their end of the bargain, the only reliable way to defend a property against a ransomware attack is to delete files and restore to the most recent backup. That said, prevention remains the best cure.

Scam School

"A hotel's first defense against ransomware is preventing it from gaining access to the property's system," said Maestro President Warren Dehan. "This can be difficult in the era of phishing scams, whereby hackers impersonate trusted sources in digital communications such as email to trick users. Phishing emails are often full of loaded links which, once clicked, are designed to provide hackers with unauthorized access to a business' systems."

Phishing scams are effective when users are busy, stressed, or unable to pay attention to small details. Unfortunately, the current hospitality and labor environment is perfect for this type of exploitation to flourish.

"Hoteliers should exercise caution when interacting with suspicious accounts, or by refusing to click on links inside email exchanges that may not be trustworthy," Dehan said. "For example, if a website sends a password change request directly to your email, users are urged to change their password directly on that website rather than navigating to the web address through any links in the email, bypassing potential attempts from hackers to steal passwords or other information. As part of your data defense initiatives, it is also important keep your antivirus up to date and stay current with operating system and network security updates."

More sophisticated scams are appearing each year, with modern hackers using publicly available information about a hotel to trick members of its staff or guests into providing them with private guest information. Known as vishing scams (voice phishing), these cons, more akin to social engineering, impersonate hotel leadership to obtain guest credit card information, phone number, email, and even home addresses by engaging in deceptive phone conversations.

"Employee training is the most crucial part of data security, as it can dissuade habits that could potentially open your property up to vulnerabilities," Dehan said. "The goal of cyber security, after all, is to make accessing your property's data more trouble than it's worth, prompting hackers to move on in search of low-hanging fruit. This is important because every hotel across the industry, independent and branded, are potential targets for cyber scams and should have a plan in place should their property's data become compromised."

Bring a Backup

If a hotel has been hacked, hopefully it has a comprehensive data storage plan in place that saves a fresh backup every night in addition to recording transaction log backups regularly throughout the day. Armed with this, a hotel could confidently delete its compromised data and restore to a backup, losing at most a handful of hours of business in exchange for cutting the

hacker loose from your system. If hotel data is hosted in the PMS provider's cloud environment, backups will be automatically done and managed, and better secured against these threats.

"It's easy to see how ransomware is a threat, but with a little extra strategizing behind their data protection strategies, hotels can be better prepared to brush these attacks aside," Dehan said. "Conversely, hotels without a way to properly retrieve or store backup data are complicating an issue that could leave them without months — or years — of data."

Dehan said hoteliers should speak with their PMS provider about setting up a data backup plan. Many of these plans can be automated, providing the confidence that hotels remain protected in the event of a ransomware attack. Thanks to data storage strategies such as these, disruptive and potentially expensive ransomware attacks can be avoided.

# # #

About Maestro

Maestro is the preferred Web Browser based cloud and on-premises PMS solution for independent hotels, luxury resorts, conference centers, vacation rentals, and multi-property groups. Maestro's PCI certified and EMV ready enterprise system offers a Web browser version (or Windows) complete with 20+ integrated modules on a single database, including mobile and contactless apps to support a digitalized guest journey as well as staff operations. Maestro's sophisticated solutions empower operators to increase profitability, drive direct bookings, centralize operations, and engage guests with a personalized experience from booking to check out and everything in between. For over 40 years Maestro's Diamond Plus Service has provided unparalleled 24/7 North American based support and education services to keep hospitality groups productive and competitive. Click here for more information on Maestro. Click here to get your free PMS Buying guide.

Barbara Worcester
PRPRO
+1 4409305770
email us here