© creativecommonsstockphotos

CYBERSECURITY AND PMS

In one of the biggest corporate data breaches in history that has left the hospitality reeling, Marriott International announced last November it had discovered a data breach dating back to 2014 on its recently acquired Starwood hotels guest reservation database in the United States. The breach could affect up to 500 million guests. *Donald Gasper* asks what the incident indicates about the state of hotel cybersecurity and looks in particular at the vulnerability of property management systems (PMS).

Marriott first learned of the breach on September 8, 2018, when a warning from an internal security device alerted the company to an attempt to access the Starwood guest reservation database. Only on November 19 was the company able to decrypt the information and determine which of its guests were affected.

For 327 million of them, Marriott says, the exposed information included their names, mailing addresses, phone numbers, email addresses, passport numbers, date of birth, gender, arrival and departure information, reservation date and communication preferences. For millions of others, their payment card numbers and card expiration dates were potentially compromised. Marriott warns that it can't confirm if the hackers were able to decrypt the payment card numbers.

While some might be shocked by the scale of this data breach, many security experts were not surprised. In fact, the hospitality industry regularly falls behind other sectors when it comes to data protection.

"Based on our analytics, the hotel industry dramatically underperforms long regulated industries such as banking and healthcare in key areas of cybersecurity," says Kelly White, founder and CEO of RiskRecon, a third-party risk management provider. "For example, in comparison with banks, hotels have a 400 per cent higher rate of critical software vulnerabilities present in internet-facing systems that store and process sensitive, regulated information. In comparison with healthcare, hotels have a 180 percent higher rate."

PMS VULNERABILITY

Hotel property management systems (PMS) are one area of potential risk, cybersecurity experts say. Whether you're a small boutique hotel or part of a large, well-known brand, your systems can be compromised, and the consequences can be damaging.

Hospitality organisations rely on a PMS for front desk and back office operations, reservations management and record keeping. As the operations hub, the PMS interfaces with or includes services and components such as point-of-sale systems, physical access control systems, Wi-Fi networks and other guest service

> Based on our analytics, the hotel industry dramatically underperforms long regulated industries such as banking and healthcare in key areas of cybersecurity
>
> *Kelly White, founder and CEO, RiskRecon*

applications. Adding to the complexity of connections, external business partners' components and services are increasingly being integrated with a PMS, such as on-site spas or restaurants, third-party booking engines and customer relationship management partners.

"This expanding PMS provides a large attack surface for adversaries," says Bill Newhouse, senior security engineer at the U.S. National Cybersecurity Center of Excellence, a collaborative hub where industry, government and academia work together to address businesses' most pressing cybersecurity issues. Part of the National Institute of Standards and Technology (NIST), the NCCoE is taking on cybersecurity challenges in various industries with a focus on applying existing security standards and guidelines to technologies available today.

"For the hospitality sector, cybersecurity and hotel technology collaborators have joined us to improve security around the PMS by building a reference architecture that follows best practices and standards in the areas of network segmentation, network control, multi-factor authentication and key management," Newhouse adds. "We are building out the architecture together, testing that it functions as expected and documenting it so that PMS owners have a working example of modular cybersecurity features they can select from as they begin to address risk."

While securing a PMS may seem like "mission impossible," opportunities exist to increase cybersecurity in and around these systems. Security situational awareness of hotel data – where and how data is accessed, moved, stored, and protected – is essential. Moreover, any tactics and tools you use to secure a PMS should be tailored to your operation and take into account your risk tolerance and your available resources. The NCCoE hospitality project, when complete, will document how to leverage existing, commercially available technologies to improve the cybersecurity of your PMS.

PROACTIVE APPROACH NECESSARY

"Security is not a destination," says Luke Pfeifer, director of PMS Product Management at Agilysys Inc. "It is an ongoing endeavour that necessitates constant attention and focus. Operators should help their employees understand this and provide ongoing, mandatory training to stress the importance of security. While all employees can be held accountable for their roles in cybersecurity, operators should designate an individual who will drive the overall security strategy and corporate protocols, performing regular testing and audits."

"It's not like you can lock your home once and never have to lock it again. What's at stake is much more than just credit card data – the personal data of every hotel guest is in jeopardy as well."

Considering the costs associated with a system breach – and its potential impact on guest privacy and brand reputation – it makes sense to take a proactive approach to securing your property management system PMS. AHOT

Bill Newhouse, senior security engineer, U.S. National Cybersecurity Center of Excellence

Luke Pfeifer, director, PMS Product Management, Agilysys Inc