NIST Publishes Guidelines Aimed at Enhancing Hotel Property Management System Security

April 27, 2021

Introduction

Hospitality organizations depend heavily on the property management system (PMS) of each hotel to run day-to-day operations. The PMS handles most vital functions, including reservations, room availability, pricing, revenue management, loyalty program integration, guest profiles, guest preferences, report generation and financial record keeping. A PMS also monitors and informs employee and guest activity, and connects with other applications such as food and beverage and amenity point-of-sale systems, central reservation systems, wi-fi and entertainment systems, sales and marketing applications, call-center databases and payment providers. As such, a PMS stores, processes and transmits a significant amount of sensitive information, including personal data and credit card data of guests, both of which are heavily regulated.

Because of the amount of data stored within a PMS and because of its interconnectivity with an organization's other systems and applications, hospitality organizations have increasingly become targets of cyberattacks, with some attacks causing significant breaches of sensitive information. These breaches have resulted in significant financial loss, an increased number of investigations, organizational disruptions, reputational damage and costly litigation. According to an industry report, in 2019 the hospitality industry ranked third among industry verticals in percent of data breaches, representing 13 percent of all breaches for that year. *See 2020 Trustwave Global Security Report*.

Recognizing that hospitality organizations could lessen the number of successful cyberattacks by increasing the security controls of each PMS, the National Institute of Standards and Technology (NIST) released NIST Special Publication 1800-27, "Securing Property Management Systems" (SP 1800-27) as a resource of voluntary guidelines for hospitality organizations to follow in order to build a more secure PMS.

Key Elements and Enhanced Security Requirements

Principal recommendations for enhancing the security of a PMS include implementing common cybersecurity controls such as zero trust, moving target defense, tokenization of credit card data, and role-based authentication. Such controls can include:

- Access throughout the organization should be role-based to prevent unauthorized access to PMS, related systems and the sensitive data;
- Access should only be provided to allowed entities (known as "allowlisting");
- Lateral movement throughout the PMS and critical systems should be disallowed;
- Credit card and transaction data should be tokenized at the outset; and
- Audits, system access logging and reporting should be implemented and maintained to raise situational awareness amongst its users.

Key Takeaways

With SP 1800-27, hospitality organizations now have an identified expectation and "industry standard" that the c-suite can use as a guide to compliance and to measure progress. By following NIST's guidelines, hospitality organizations will be able to limit exposure of a PMS to incidents in systems that interface with it and demonstrate that the organization was following industry standard practices should a breach occur.

Hospitality organizations that want to increase the security of their systems and data need to start by mapping their cybersecurity controls and conducting a risk assessment to identify threats and vulnerabilities. Such assessments should be conducted in conjunction with experienced counsel to assist with understanding the risk profile for the organization and preserving privilege when possible.

If you have any questions regarding NIST Special Publication 1800-27 or any other aspect of your data protection and security practices, please contact any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.