NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SECURING PROPERTY MANAGEMENT SYSTEMS

Cybersecurity for the Hospitality Sector

The National Cybersecurity Center of Excellence (NCCoE) is helping hospitality organizations implement stronger security measures within and around their property management system (PMS) through collaborative efforts with industry and the Information Technology (IT) community, including vendors of cybersecurity solutions. This fact sheet provides an overview of NIST Cybersecurity Practice Guide SP 1800-17, *Securing Property Management Systems*. If you have feedback on the architecture or the relevance and usefulness of this practice guide, please contact us at hospitality-nccoe@nist.gov.

BACKGROUND

In recent years criminals and other attackers have compromised the networks of several major hotel chains, exposing the information of hundreds of millions of guests. Breaches like these can result in huge financial loss, operational disruption, and reputational harm, along with lengthy regulatory investigations and litigation. Hospitality organizations can reduce the likelihood of a hotel data breach by strengthening the cybersecurity of their property management system (PMS). The PMS is an attractive target for attackers because it serves as the information technology operations and data management hub of a hotel.

CHALLENGE

Hospitality organizations rely on a PMS for daily tasks, planning, and record keeping. As the operations hub, the PMS interfaces with several services and components within a hotel's IT systems, such as point-of-sale (POS) systems, physical access control systems, Wi-Fi networks, and other guest service applications. A PMS and its extended systems store, process, and transmit a variety of sensitive guest information, including payment card information and personally identifiable information. An unsecured or poorly secured PMS could expose a hotel–and the larger hospitality organization of which the hotel is a part–to a significant and costly data breach, which may result in financial penalties for violating state, federal, and international privacy and other regulatory regimes.

APPROACH

This cybersecurity practice guide shows an approach to securing a PMS and the system of guest services it supports. It offers how-to guidance for building a reference design using commercially available products within a zero trust architecture to mitigate cybersecurity risk that includes role-based access control, privileged access management, network segmentation, moving target defense, and data protection.

BENEFITS

The potential business benefits explored by this project include:

- **instill consumer confidence and brand loyalty** by protecting guest privacy and payment card information
- **limit the cost** for recovery and mitigation if a breach occurs
- **build the business case**, functional requirements, and test plan for a similar solution within your own environment
- **support privacy/regulatory compliance** by using data tokenization and limiting the spread of data beyond "need-to-know"
- **increase overall PMS security** situational awareness, and limit exposure of the PMS to incidents in systems that interface with it
- **control and limit access** to your PMS to those with a business need

DOWNLOAD THE GUIDE

For more information about this project, visit: https://www.nccoe.nist.gov/projects/use-cases/securing-property-management-systems

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have questions about this project please email hospitality-nccoe@nist.gov.

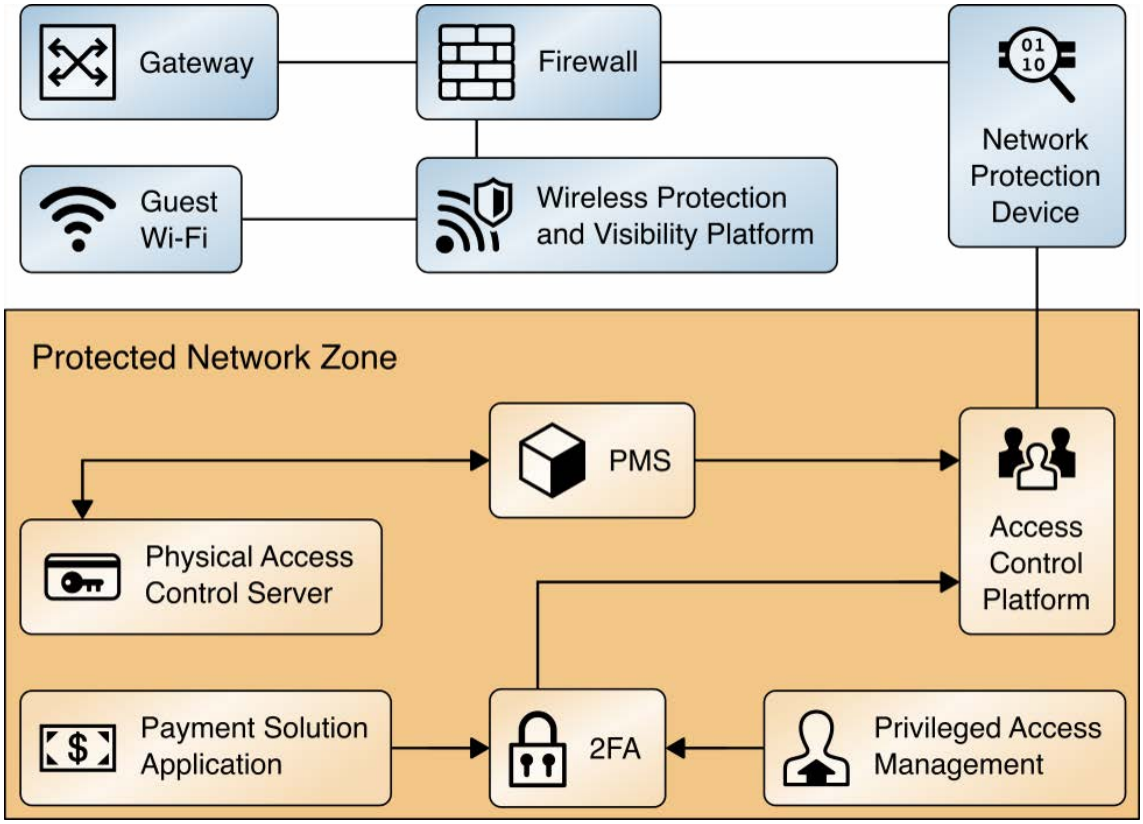
COMPONENTS

To better secure the PMS, an example solution may include, but is not limited to, the following components and zero trust tenets:

- Property Management System
- Network Protection Device
- Access Control Platform
- Privileged Access Management
- Wireless Protection and Visibility Platform
- Payment Solution Application
- Physical Access Control Server
- Firewall

- All data sources and computing services are considered resources
- All communication is secured regardless of network location
- Access granted on a per session basis
- Access granted based upon dynamic policies
- Ensure all devices are in the most secure state possible
- Constant cycle of access, scanning and assessing threats; adapting and continually reevaluating trust for all resources, as authentication and authorization are dynamic and strictly enforced before access is allowed
- Continuous collection of data on the state of devices, infrastructure and communications

HIGH-LEVEL ARCHITECTURE



TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors who are participating in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution. Technology collaborators on this project include:

CRYPTONITE NXT · FORESCOUT · HÄFELE · Remediant · STRONGKEY · tdi technologies

Certain commercial entities, equipment, products, or materials may be identified in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE ABOUT NCCOE
Visit https://www.nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

March 2021