WPP license no. MR/TECH/WPP-73/North/2017 License to post without prepayment Postal Registration No. MCN/98/2015-2017.
Published on 4th of every month. Posting date: 6th & 7th of every month. Posted at Patrika Channel Sorting Office, Mumbai-400001.
Registered with the Registrar of Newspapers under RNI No. MAHENG/2009/34648.

Total pages 112

Volume 9 | Issue 8 | September 2017 | ₹50

hotelier india

THE DEFINITIVE GUIDE TO SUCCESSFUL HOTEL MANAGEMENT

www.hotelierindia.com

POWER LIST 2017

CELEBRATING EXCELLENCE IN THE HOSPITALITY INDUSTRY

Published by ITP Media (India)

FIX YOUR RISK

An important issue in contemporary times, when it comes to hotels, data security needs to be addressed even more diligently since it involves guests' security and their privacy

BY BINDU GOPAL RAO

Data threat is not limited to credit card forgery but also cyber-attacks on guest network and hotel network.

Most customers never give much though to the fact that hotels take so much of their personal data including their credit card details when they check in. That is probably because they have implicit trust in the hotel's security practices when they volunteer this information.

However, if the thought every crossed their mind that this data could be compromised, would they be willing to part with it while checking in? Would they even want to stay in a hotel if they ever learn that it had suffered a data breach in the past?

Can you see how easily the spotlight has been firmly affixed on the data security systems implemented in hotels? And also why it is imperative for these to be robust, scalable and be able to thwart all kinds of potential attacks.

The hospitality industry has witnessed numerous sophisticated attacks on secured data including the recent breaches reported by InterContinental Hotels Group and Sabre Hospitality Solutions. It is not surprising, but hackers have usually targeted the payment card data information from different point-of-sales (POS) systems in hotels resulting in unauthorised credit card charges and other malicious activities.

Apart from the lack of POS encryption; hotel networks are often poorly defended in some cases allowing hackers to sit undetected on networks. The industry has witnessed also hackers increasingly moving to ransomware and extortion, a modus operandi that is spreading like wildfire in other industry sectors as well.

KEY THREATS

Data threat is not limited to credit card forgery but also cyber-attacks on guest network and hotel network. Hotels need to think about multiple endpoints and remote connections they rely on to run the property's operations. Electronic door locks, HVAC controls, alarms and a full range of Internet of Things (IoT) devices can fall under the control of cybercriminals aiming to disrupt normal operations, highjack data and misuse it. Hotels accommodate diverse, global clients and corporate travellers with high-credit worth. They are favourite targets for cybercriminals due to the availability of massive number of potential credit cards at one location and large amount of customer data.

Subhendu Sahu, acting country manager for India, FireEye pointed out

"Keeping all our data security standards and implementation in place, we ensure that its usability is simple for guest devices, where most security protocols run at the backend with little or no intervention"

– Bijesh Mukundan, IT manager, Le Meridien Mahabaleshwar Resorts and Spa

CYBERCRIME IS THE MOST PREVALENT IT THREAT ACTIVITY FACED BY THE HOSPITALITY SECTOR.

that cybercriminals often attack hotels through spear-phishing emails to deliver malware and extortion tactics. They are typically focused on stealing credit card information and personally identifiable information. Most of these actors are opportunistic and generally seek isolated systems for exploitation. They tend to go after large volumes to be sold in the underground. Another threat is cyber espionage. "Business and government professionals, especially to visiting foreign countries, often rely on hotel networks to conduct business and may be unfamiliar with threats posed while abroad. Last month, we observed a campaign by threat group APT28. This Russia-based group compromised hotel Wi-Fi networks to steal personal credentials of hotel guests," Sahu added.

SAFE AND SECURE

Organisations need to be able to detect and respond to unique attacks that have not been seen before and the key is to have strong coverage on a network's endpoints – whether those are POS, workstations, or mobile device. Hotels are vulnerable to cybercrimes through a variety of avenues that break with the traditional physical security measures deployed across the hospitality industry.

According to Gaurav Tyagi, IT manager of StayWell Hospitality Group India regular monitoring of network should be conducted to identify irregular activities. One cannot put the entire responsibility on a machine and relax as machines can perform its task but someone ought to monitor it withing its parameters. "A security threat could come from a hotel guest too. To avoid this, use two different networks and keep them physically separate. Using a good quality firewall on both these networks helps. We normally avoid giving internet access on staff's personal computers and avoid it on official computers if it is not necessary," he added.

Sarada Muduli, revenue manager, Lords Hotels & Resorts stated that his hotel chain has installed a WiFi firewall that alerts his team about any compromise to its operations. The company also has an auto trigger for anti-hacking, anti-spamware, and antivirus to protect email communication of guest database.

"We try and keep the interface for the guests very simple, however since it is a sensitive area we maintain standard protocols like mandating an OTP while signing into the hotel's WiFi or a personalised check with PMS. While this might be slightly intrusive, guests are aware of its reason. We also request them for identity proof and offer secured platform to them to use the facilities," Muduli revealed.

Hotels need to be able to detect and respond to unique attacks by having strong coverage on their network's endpoints.

"The IT team should run drills periodically to test the system's efficiency and preparedness. This allows them to identify any loopholes and rectify them promptly."

– Sarada Muduli, revenue manager, Lords Hotels & Resorts

PRIVACY ISSUES

A key aspect in hotels is ensuring that guests are not inconvenienced at any time and their security measures are discreet. "Keeping all our data security standards and implementation in place, we also ensure that its usability is simple and straight forward for the guest devices, where most of the security protocols run at the backend with little or no guest intervention," explained Bijesh

"No security software, anti-virus system or other tools can offer 100% guarantee to prevent cyber-attacks."

– Thirupati Gasiganti, IT manager, Novotel Hyderabad Airport Hotel

Mukundan, IT manager of Le Meridien Mahabaleshwar Resorts and Spa. For instance, guest authentication is taken only as and where crucial, and all guest personal data is wiped out post-guest usage automatically on public access devices.

Before seeking any data security solutions, hoteliers are required to undertake the shift in the mind-set and recognise that in today's scenario, cyber breaches are not a question of 'if' but 'when'. "Without graduating from breach-denial or breach-prevention only to breach-acceptance, hoteliers would not be able to see the right solutions that safeguard them as well as their guests against the challenges in the cyber-age. As they undertake this mind-shift, the realisation to change their security strategy to make it data-centred shall be a natural choice. Having said that they need to review the three-step secure-the-breach strategy to protect the data through encryption, secure key management and strong multi-factor authentication," explained Rana Gupta, VP, APAC, Sales, Identity and Data Protection, Gemalto.

> "Without graduating from breach-denial or breach-prevention only to breach-acceptance, hoteliers would not be able to see the right solutions that safeguard them as well as their guests against the challenges in the cyber-age."
>
> **– Rana Gupta, VP, APAC sales, identity and data protection, Gemalto**

THE RIGHT FIT

Implementing the best payment gateway, secured booking engines, firewall for WiFi internal usage and external firewalls are some ways to safeguard sensitive data. While numerous solutions are available to maintain data privacy, it is important to bear in mind that these are scalable.

"No security software, anti-virus system or other tools can offer 100% guarantee to prevent cyber-attacks. On the other hand, securing and limiting the system too much may cause other problems such as preventing customers from accessing information they might need. Thus, hotels should manage the risk in cyber defence in a meaningful manner that has a balance in security implementation using the newest technology available while testing the security posture by using strong feedback structure," said Thirupati Gasiganti, IT manager at Novotel Hyderabad Airport Hotel.

Practices like creation of separate networks for each aspect of the hotel helps in preventing cyber criminals from gaining wider access to more vulnerable networks. Hotels, therefore, are implementing innovative strategies to safeguard their data and also protect customer information.

"Segregating sections in different VLANS is already in place. However, people still play a vital role. We have enforced no-removable device policy in our network with exception to only IT and the secure BIOS, disallowing any boot configuration alteration. Also, we have secure LAN ports disallowing any foreign device connection physically," he stated.

PROTOCOL MATTERS

Technology companies have their own list of protocols that they advice hoteliers to follow. "Companies should have end-point and email protection to detect the advanced forms of the attacks, such as spear phishing emails that contain malicious macros to launch malware that can steal credentials or serve as a beach head on a system. It is vital for organisations to have the right threat intelligence to understand how other countries employ these tactics. In cyber, tactics move at the speed of a click. Other countries and criminals adopt malware and tactics of another country," opined Sahu.

Muduli added, "The IT team should run a drill periodically to test the system's efficiency and preparedness. This allows them to identify any loopholes or errors and rectify them promptly. Fronts such as the website domains need to be up and running at all times and so it is auto responsive to any cyber-attack."

SINCE 2013, AS PER THE BREACH LEVEL INDEX, THE HOSPITALITY SECTOR HAS WITNESSED OVER 57 DATA BREACHES THAT LED TO ALMOST 10.5 MILLION DATA RECORDS BEING COMPROMISED WORLDWIDE.

NUMBER CRUNCHING

Data security solutions are quite expensive and based on the business requirement a specific budget allocation is required. Tyagi said, "We have to look it in to two parts -things which are necessary to run the business and things which must be there from IT point of view. In hospitality industry, management is more interested in first part but as an IT person you cannot ignore the latter. For example, you can easily get budget to improve your Internet speed, but it is very hard to get approval on firewall upgrade."

Naturally then ensuring that hoteliers are able to make a wise investment in arguably the most important aspect of data security. It is of paramount importance in an industry where the key differentiator will be guest trust and confidence.

> "Last month, we observed a campaign by threat group APT28. This Russia-based group compromised hotel Wi-Fi networks to steal personal credentials of hotel guests."
>
> **- Subhendu Sahu, Acting Country Manager for India, FireEye**