VIEW POINT

IMPLEMENTING MULTI-LAYERED SECURITY FOR HOSPITALITY BOOKING PLATFORMS

Abstract

Hotel booking platforms store sensitive customer data, making them prime targets for cyberattacks that can cause severe financial and reputational damage. A study across 24 countries found that 38% of data breaches occurred in hotels, with 98% involving stolen credit card information. To mitigate these risks, IT admins and cybersecurity professionals advocate a multi-layered security approach, which safeguards critical assets against various threats. This article explores common cyber threats, protection strategies, and the benefits of a layered security approach.

Infosys®
Navigate your next

Common cyber threats hotel booking platforms face

Hotel booking platforms hold critical customer data, including their past, current, and future booking schedules, phone numbers, passport details, credit card details, and much more. Due to this, their systems and databases are lucrative targets for malicious actors.

Malware

Malware, such as viruses and ransomware, are the most common and dangerous threats to online hotel booking platforms. They pose a direct threat to the security and integrity of the reservation system and the website.

Spam

Unsolicited advertising emails that fill up the drive space and often contain malware are designed to be very tempting to open. The staff requires regular training to be aware of such emails that ask for personal and financial information.

DDoS attack

In a DDoS attack, a hacker overwhelms the server with excessive traffic, causing it to crash and preventing legitimate users from accessing the platform. High-profile websites such as hotel booking engines are prone to such attacks.

Ransomware

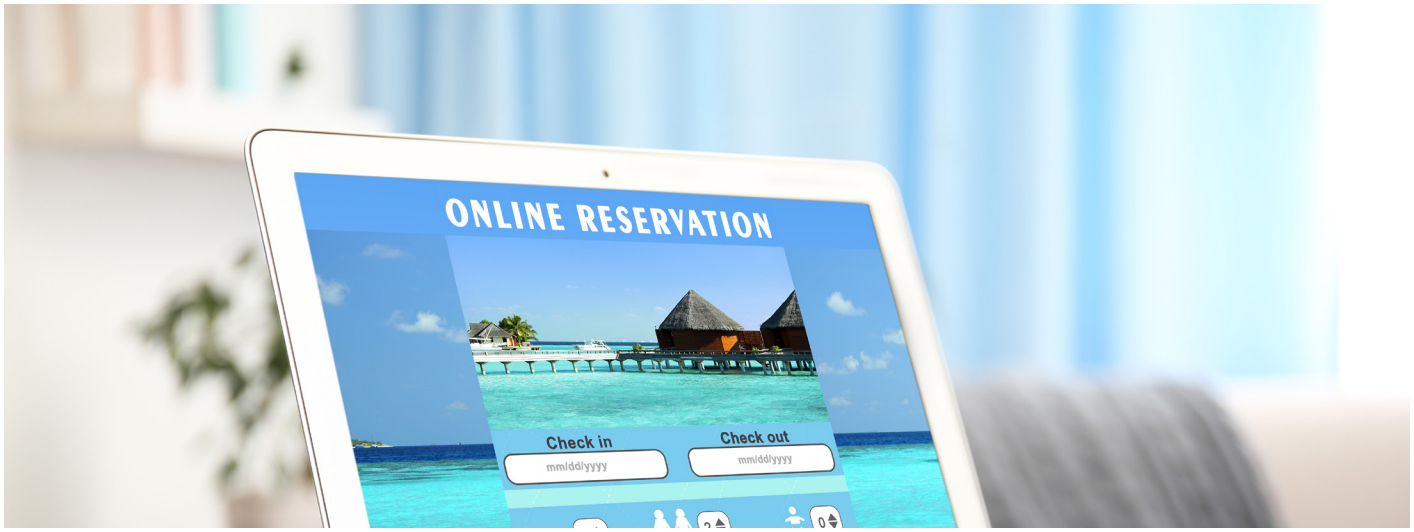
A ransomware attack locks users out of their data, systems, or networks until a ransom is paid. The miscreant holds the organisation for ransom. In some cases, hotels have paid several thousand dollars to regain control of rooms to release the guests who were locked in. Similar attacks could happen on the booking platform, barring customers from completing the booking and forcing the hotel to lose significant revenue.

Payment card theft

Hotel booking platforms rely on integration with third-party credit card or debit card payment systems for quick bookings. This makes them prone to attacks due to a weakness in the credit card company's systems.

Ways to ensure the security of hotel booking platforms

Booking platforms can implement these hospitality security measures to ensure that their customer data is safe:



PCI DSS compliance

The Payment Card Industry Data Security Standard (PCI DSS) protects the hotel booking platform and stores and transmits the credit card information in a secure environment. PCI DSS-compliant merchant account processes the payments through a secure server and ensures the safety of online financial transactions for booking hotel rooms.

HTTPS secure website

An SSL-encrypted website keeps the customer data, including payment details, safe. A secure website displays it in its URL as https://, which Google also prefers over unsecured websites. Studies have shown that 84% of online customers would abandon the cart if SSL did not secure the website. If a hotel booking platform wants more direct bookings and wants to remain at the top of Google search ranking, it must use HTTPS.

Web application and API protection (WAAP)

WAAP services protect the application from hidden vulnerabilities which can allow entry to a hacker. This, along with a Web Application Firewall (WAF) blocks malicious traffic and prevents attacks from bots.

Secure payment gateway

Third-party secure payment gateways keep the payments secure for a small percentage of each transaction. Property booking management systems must integrate well with a third-party secure payment gateway to protect the customer. Additionally, the payment should give an attractive currency conversion rate and 24/7 customer support.

GDPR implementation

General Data Protection Regulation (GDPR) started in Europe but has quickly become the data security standard for the whole world. Ensure that the online booking platform runs on a GDPR-compliant website and that there is explicit consent from the guest before collecting their personal information.

Cybersecurity protocol review

A regular review of the booking platform's hospitality security issues and weak spots protects businesses from losing reputation and customer business. Such a multi-layered security review may include:

1. Re-evaluate the security of the data encryption algorithm
2. Review Multi-Factor Authentication (MFA) and role-based access
3. Evaluate the network security, including wi-fi and firewalls
4. Check the security compliance of third-party platforms
5. Impart the cybersecurity training to all the team members regularly

The value of layered hospitality security

In a rapidly changing landscape for platform security, a single line of defence is not enough. By implementing multi-layered security, hotel booking platforms can protect their clients better:

Human layer

This layer is the staff that operates and maintains the hotel booking platform. They are vulnerable to keeping weak passwords and phishing attacks, which may compromise the client's security. Businesses can secure this layer through regular training and building a culture of security awareness.

A key challenge to securing this layer is to ensure that the employees are up-to-date and the training material remains effective over time. Regular security awareness training covers social engineering attempts, practising good password hygiene using two-factor authentication (2FA)/multi-factor authentication (MFA), and reporting an incident.

Perimeter security

Perimeter security forms a barrier between the organisation's network and systems and the outside world. One of the challenges of permitter security is to manage the traffic volume and complexity. Perimeter security becomes more challenging as organisations adopt cloud services.

Firewalls are the fundamental component of perimeter security. It controls the traffic and protects the hotel booking platform based on predefined rules. Next-generation firewalls (NGFWs) come with application awareness and threat intelligence. Additionally, intrusion detection and prevention systems raise alerts and block malicious traffic, and Virtual Private Networks (VPNs) provide secure access by encrypting the transmitted data.

Network security

The network security layer protects the integrity, confidentiality, and availability of data on the network from unauthorised access and cyber threats. Geographically diverse networks in large hotel chains or global hotel booking platforms can be challenging to protect due to lesser visibility and control over network traffic and endpoints.

However, multi-layered security systems can divide the network into multiple Virtual Local Area Networks (VLANs) to monitor and control the flow of traffic. Security Information and Event Management (SIEM) systems analyse data from multiple devices and respond to threats in real time. Lastly, penetration testing and vulnerability assessment can identify and address potential weaknesses in the network the hotel booking platform runs on.

Endpoint security

As the name suggests, endpoint security protects user devices such as laptops, mobile phones, and computers from cyber threats. Each endpoint device is a potential entry for attackers who want to access the booking platform backbone.
In large hotel booking platforms that work globally, managing each device's security can become challenging. However, with the help of the right tools, businesses can monitor, update, and protect each device's security protocol. These may include anti-virus software, anti-malware tools, and Endpoint Detection and Response (EDR) solutions.

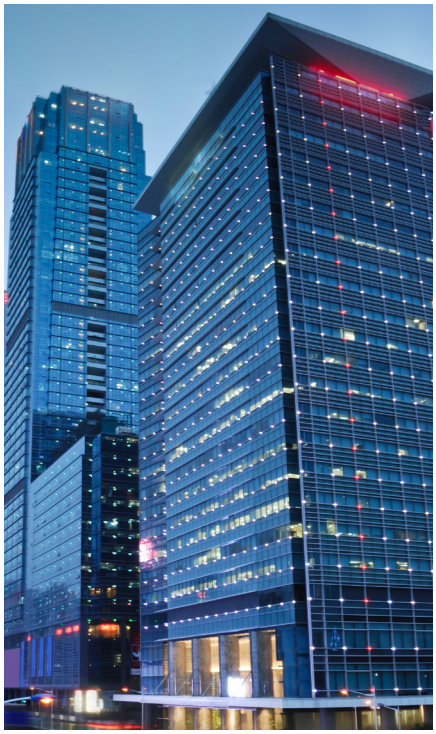
Application security

Protecting the software applications that form the baseline for hotel booking platforms from threats and vulnerabilities is crucial. High-quality coding practices and regular assessments help secure the applications, business-critical data, and its users. This layer also covers user authentication and access to third-party applications. Secure password policies can significantly reduce the risk of credential theft.
When developing a hotel booking platform in-house, consider integrating these practices through agile and DevOps methodologies to balance out the need for security without compromising the release cycle.

Mission critical assets security

Mission-critical assets for a hotel booking platform could include cloud servers, networking equipment, and end-user systems. Protecting these assets must ensure that all potential threats are neutralised without disrupting critical operations or access to the hotel booking platform for the customer. One can achieve this through redundant systems and failover mechanisms.

Data breach case studies in the hospitality sector



In 2018, Marriott International, an international chain of hotels, faced a massive cyber attack in which criminals compromised the reservation system, stealing the data of millions of customers across countries. This data included Marriott's current and past customers who stayed with the hotel. As a result, Marriott Group faced significant expenses for data recovery, legal ramifications, and reputational damages.
The system vulnerability was introduced during Marriott's acquisition of Starwood in 2016, which highlights the need for prioritising cybersecurity during M&As. Miscreants initially infiltrated the guest reservation system of Starwood in early 2014 using a Remote Access Trojan (RAT), granting the perpetrator unauthorised access to the technology. Some of the hotel's properties were using outdated versions of Windows Server and had left the remote access ports open to the internet.
During the acquisition, Marriott failed to identify that Starwood's systems were already compromised, and the cybercriminals managed to remain undetected during the acquisition process. Marriott finally confirmed that the personal information of 500 million customers around the world was stolen. This included names, addresses, email addresses, phone numbers, passport numbers, and credit card numbers.
As a result, Marriott Group incurred a $30 million recovery expense, its shares dropped by 5%, and the company suffered a loss of $1 billion in revenue due to the reputation damage.

End note

Multi-layered security in hotel booking platforms is a critical factor that protects hospitality businesses from financial and reputational damage. By adopting the technologies mentioned above, businesses can take a multi-layered approach to network security, data protection, endpoint security, PCI DSS compliance, physical security integration, and engineering awareness.

Lastly, proactive risk assessments, staff training, continuous monitoring, and staying up-to-date with emerging threats are essential for multi-layered security in hotel booking platforms.

For more information, contact infosysbpm@infosys.com

Infosys®
Navigate your next