Modernizing pentesting: strategies for leisure and hospitality

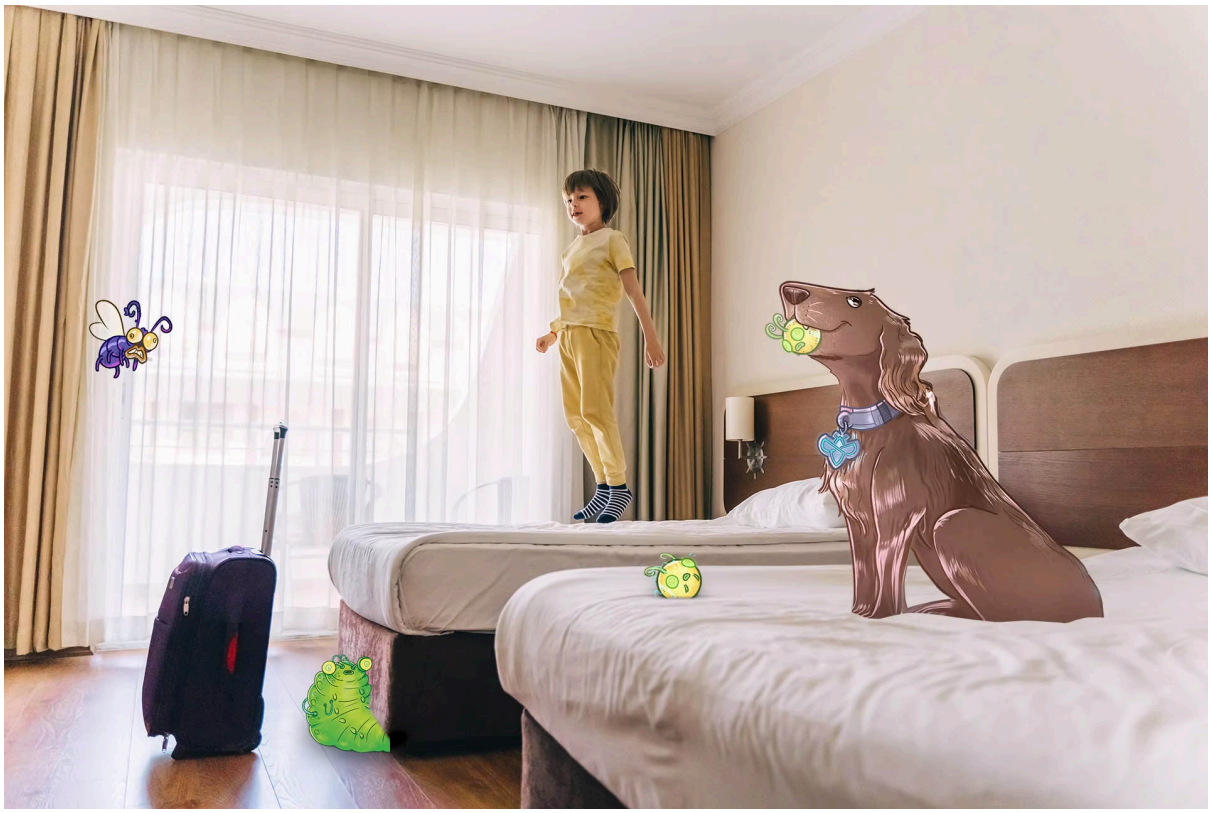
BY ANNA HAMMOND · MARCH 11, 2024 · LAST UPDATED ON AUGUST 8, 2026

Want to read the latest version? Visit the link below:
https://www.intigriti.com/blog/business-insights/modernizing-pentesting-strategies-leisure-and-hospitality

Technology is changing how the leisure and hospitality industry works as it becomes more reliant on Internet of Things (IoT) devices. But with new technologies comes new threats. These devices can be vulnerable to attacks and can provide a gateway for malicious actors to access sensitive guest data. In this industry, pentesting is a crucial tool for cyber resilience. It helps organizations find and fix security weaknesses before they can be exploited.

This article will delve into the distinctive benefits and limitations for security testing in the leisure and hospitality industry. We also explore evolving pentesting techniques that can help organizations achieve cyber resilience.

The unique cybersecurity challenges of the leisure and hospitality sector



Travel and leisure organizations can protect customer data through regular security testing, ensuring family trips are secure in all respects.

The digital landscape is rapidly changing the leisure and hospitality industry as IoT devices and interconnected systems are being widely implemented. Examples include Point of Sale (POS) payment systems, smart locks, and in-room entertainment systems, which improve both guest satisfaction and operational efficiency. However, this also increases the risk of cyber threats, as the industry's attack surface expands.

One of the biggest cybersecurity challenges for the leisure and hospitality industry is the handling of sensitive guest data. Personal information, credit card details, and travel itineraries are all valuable targets for cybercriminals. A data breach can not only damage a company's reputation but also result in financial losses and legal liabilities.

Another challenge is the industry's reliance on legacy systems and outdated software. Many hotels and hospitality businesses still operate on old IT infrastructure that may not have been designed with modern security threats in mind. These systems are often vulnerable to exploits and may not receive regular security updates, making them easy targets for attackers.

Finally, the distributed nature of the industry, with multiple locations and remote access points, complicates the implementation of consistent security measures. Ensuring that all properties and systems are adequately protected can be a significant challenge, especially for large hotel chains or hospitality groups.

Pentesting: A critical tool for cyber resilience

Pentesting has become widely recognized as a key factor in enhancing cyber resilience for the leisure and hospitality industry. This proactive approach involves simulating cyberattacks to uncover vulnerabilities before malicious actors can exploit them. By identifying and addressing these weaknesses, businesses can significantly reduce the risk of data breaches, financial losses, and reputational damage.

Leisure and hospitality organizations should prioritize key areas to test, such as:

- Guest data management systems
- Payment processing systems
- Access control mechanisms.

Given the increasing reliance on IoT devices and interconnected systems, testing their security becomes paramount to preventing cybercriminals from exploiting these entry points.

Regularly conducting penetration testing enables organizations to maintain compliance with industry regulations and standards like PCI DSS and GDPR. This not only ensures adherence to legal requirements but also fosters trust among customers and partners. In turn, this can translate into increased revenue and sustained success in a competitive market.

5 limitations of pentesting for leisure and hospitality businesses

Pentesting, while important, has limitations for leisure and hospitality organizations. To make informed decisions and enhance their security, its important that businesses acknowledge and address these. Here are five key limitations:

1. **Limited scope:** Pentesting focuses on specific systems, leaving potential blind spots in the interconnected infrastructure of the leisure and hospitality industry.

2. **Time constraints:** The fast-paced nature of the industry makes it challenging to conduct regular pentests, leaving organizations vulnerable to emerging threats.

3. **Lack of real-world simulation:** Conducting pentesting in controlled environments might not fully capture the real-world challenges faced in the industry. This can create a false sense of security.

4. **Human error and bias:** Testers can overlook vulnerabilities or fail to consider unconventional attack vectors, introducing subjectivity and inconsistency in results.

5. **Incomplete remediation:** Pentesting identifies vulnerabilities, but organizations may struggle to promptly address them, leaving a window of opportunity for attackers.

To overcome these limitations, organizations should complement pentesting with evolving security testing techniques to build a robust security posture.

Evolving security testing techniques for the leisure and hospitality industry

One notable evolvement in security testing for leisure and hospitality companies is the implementation of crowdsourced pentesting. This is where organizations engage a community of ethical hackers to identify vulnerabilities from diverse perspectives. This approach complements traditional pentesting methods by leveraging the expertise of a broader pool of security professionals. You can kickstart this approach through Intigriti's Hybrid Pentest solution.

Furthermore, the industry is embracing continuous pentesting, recognizing the dynamic nature of cyber threats. An example of this is bug bounty programs. This approach involves ongoing testing throughout the year, rather than relying solely on periodic assessments. Continuous pentesting ensures that organizations remain vigilant against emerging vulnerabilities and can promptly address any security gaps.

Regardless of the chosen approach, implementing a robust patch management system is crucial for organizations. Having one in place will ensure timely installation of security updates for their software and systems.

Achieving cyber resilience through continuous security testing

Regularly conducting vulnerability assessments and penetration tests is crucial for identifying potential security gaps. Finding these issues promptly also empowers security teams to implement timely remediation measures. By adopting these continuous security testing practices, the leisure and hospitality industry can enhance its overall cyber resilience.

To learn more about bug bounty programs and pentesting for financial services, get in touch