CYBERSECURITY THREATS FOR HOTELS – HOW TO PROTECT YOUR SYSTEM

Security is key for accommodation facilities. However, it has many different forms. Now that the pandemic has prompted a very specific type of security, biosecurity, hotels run the risk of forgetting the alarming issues of hotel cybersecurity. That involves all those problems that arise from digitization and the use of certain tools.

The Hotel Technology and Security Risks report analyzes the pros and cons of maintaining the existing technology. It also assesses the financial and security risks associated with modern hotel technology, specifically PMSs (property management systems).

Hotel Cybersecurity Issues

To understand what we are up against, we first have to take into account that **security breaches have increased by 11% since 2018 and 67% since 2014.** Therefore, according to Accenture data, it is a real risk that could continue to grow in the future. Especially in a sector that handles as much data as the hotel industry.

In the end, establishments have to control sensitive information, such as data associated with credit cards or national identity documents. In other words, they have to be vigilant. Especially since, according to a study carried out by Security Boulevard, 9% of U.S. citizens over the age of 18 have suffered a data breach during a hotel stay.

The statistics are undoubtedly worrying. Hence, cybersecurity has become increasingly important. The debate revolves around the privacy regulations to be adopted... such measures have already caused some recent problems. Moreover, in the future, they could pose a greater challenge, as higher fines have begun to be imposed for data breaches.

Causes of Digital Security Breaches

According to a report by the Ponemon Institute, it takes an average of 197 days to discover a security breach. This is undoubtedly far too long. On top of that, you have to add the 69 days it takes to fix it. In that time the losses to the victim can be incalculable.

The report uses as an example a 500-room hotel with an average stay of two nights and two guests per room. A quick calc shows that by the time everything is sorted out, it will be too late. By then, the data of 150,000 customers will have been exposed and they will have lost confidence in the brand.

Again, going to the data, the reality is that it has been proven that 95% of security breaches are the result of human error. While this may seem reassuring, it should not be forgotten that technology can prevent breaches in the first place. In that sense, making a good choice of the tools to be used is a way to gain peace of mind and avoid unnecessary risks.

The Importance of a Good PMS

It should not be forgotten that, due to the large amount of sensitive data they contain, PMSs are among the favorite targets of hackers. As a result, the U.S. National Institute of Standards and Technology (NIST) has recently published a 224-page document containing a list of recommendations on how to secure PMS.

Therefore, it is demonstrated that now more than ever, choosing good PMS is essential for the proper functioning of the hotel. Due to their long-life cycle, they usually last almost a decade, so it is better to spend those years with a good ally on your side. That is to say, before changing it, it is advisable to evaluate the different options very well.

If the current one does not provide enough confidence, you can think about replacing it sooner. However, a priori, the prospect of changing it prematurely can also be overwhelming, since it's quite expensive. Not only financially, but also in terms of the cost of retraining employees and the loss of data that is likely to be incurred.

Nor should we lose sight of the fact that legacy solutions are more exposed to cybersecurity breaches, due to their infrastructure. This is what happened a few years ago with the Marriott hotel chain, which suffered a cyberattack that exposed the personal information of 500 million customers. Therefore, leaning towards a cloud-based system can help prevent the problem.

Keeping Data Safe in the Cloud

It must be essential for the hotel to keep customer data safe at all costs. Personal information must be treated with extreme care to avoid privacy violations. Hence, the cloud becomes an ally. It should be remembered that in the case of older systems, all customer data is stored on-site, physically on a computer in the accommodation.

Since it is often stored in a place where your employees can easily access it, data could be in potential danger. It would be enough to get access to a USB port to steal years of sensitive data. Meanwhile, in the cloud, there would be no way to get them. Instead of at the hotel itself, the information is stored in strictly controlled locations, such as an AWS data center in your country or region. Choosing a provider based on its compliance with data sovereignty laws is ultimately crucial to protecting information.

Another advantage of cloud-based systems with a microservices architecture is that they can be better integrated with third-party solutions. Thus, modern PMSs are more like hubs than end-to-end systems. At the same time, the use of APIs allows hoteliers to connect other programs and tools as needed, without high integration costs and long development queues.

Experts argue that hoteliers should at least have the opportunity to test the technology before implementing it. Otherwise, there is a high risk that they may end up being slaves of their own PMS, even if it is limited.

The Risks of Investing in New Technologies

Beyond the security risks, choosing the wrong system could affect hotel operations and customer experience. For example, it has been studied how the implementation of cleaning applications reduces labor costs while increasing productivity by up to 20%. However, most PMSs neither offer the module nor allow integration with third parties involved in the cleaning processes.

Similarly, creating an RMS or offering online registration is not always possible. **The study even claims that most hotels offer a worse technology experience than what travelers get at**

home. They point out the very negative impact this has on the guest, which translates into a bad reputation and lower revenues.

Therefore, most experts believe that the cost of implementing new solutions will be considerably less than continuing with their current technology stack, only to end up with unusable and unstable systems within five years. By making decisions with this mindset, cybersecurity issues can be reduced in the future, as well as fines resulting from breaches.

Date: 2022-03-28

Article link:
https://www.tourism-review.com/cybersecurity-has-become-a-crucial-issue-for-hotels-news12457