Info Guide

Cybersecurity and the hospitality industry

Overview

- **Hotels were the third most targeted industry in 2019.**
- **The hotel industry is considered an easy target, by hackers.**
- **423 million tourists in the United States have been victims of a cyberattack as a result of their dealings with hotels.**
- **70 percent of hotel visitors say that the industry does not spend enough in cybersecurity protection.**

Tackle hospitality's biggest threat.

In recent years, attackers have gained access to the networks of numerous big hotel chains, revealing the personally identifiable information of hundreds of thousands of customers each time. In 2019, the hotel business placed third among the industries that were penetrated by cybersecurity breaches, accounting for 13 percent of the overall number of incidents. Attacks against corporate servers, which frequently hold visitor information and interface with on-site property management systems, accounted for around two-thirds of all breaches in 2014. Exposure of this nature can have a negative impact on a company's reputation, cause activities to be disrupted, and result in significant financial loss.

The hotel industry, like the majority of other businesses that are often targeted by hackers, is considered an easy target. An investigation into hacker forums indicated that the hotel companies Hilton and Marriott were mentioned in conversations about simple targets in 31 percent and 28 percent of instances, respectively.

Furthermore, it is supported by the data on the ground. To date, 423 million tourists in the United States have been victims of a cyberattack as a result of their dealings with hotels. In addition, 70 percent of hotel visitors say that the industry does not spend enough in cybersecurity protection.

So, what exactly is going wrong?

According to a breakdown of hotel data breach sectors, 64 percent of breaches occur within company internal networks, and 18 percent occur in both e-commerce and point of sale. This shows that staff education and inadequate cyber hygiene are the primary causes of the problem in the hotel industry.

Top 3 threats to hospitality organizations.

Phishing

Phishing is the practice of sending and receiving emails that appear to originate from a legitimate source. It is used by criminals in order to persuade the receiver that he or she should disclose information with them. This fraud, which frequently involves the theft of passwords and financial information, is one of the oldest on the internet.

In recent years, this danger has grown in sophistication, with attacks increasingly directed at persons in positions of control. To do this, a user's email account is compromised and fraudulent emails are sent to coworkers. Most of the time, these emails are intended to persuade recipients to authorize transactions that have been directed from above.

Ransomware

The most well-known of recent ransomware outbreaks, known as WannaCry, targeted countries and businesses all around the world at the same time. WannaCry, the most recent ransomware attack, posed a serious threat to the public by encrypting data and gaining control of some computers. The goal of this attack was to profit financially from individuals who agreed to pay the necessary sum in order to have their data/systems restored.

In your capacity as a hotelier, you are particularly vulnerable to cybersecurity failures that allow this type of assault to take place. Hotels who have fallen victim to this fraud have in the past paid more than $17,000 to be able to admit guests into their rooms and to produce electronic keys for their guests to use.

DarkHotel Hacking

Not familiar with the term DarkHotel? It is a relatively new one, which sees criminals use a hotels Wi-Fi to target business guests.

The attacks use forged digital certificates to convince victims that a software download is safe. To enable this to happen criminals upload malicious code to a hotel server, and can then target specific guests. The first instance of DarkHotel hacking was first seen in 2007 and originated via peer-to-peer networks and spear-fishing scams. If you have guests that are concerned about DarkHotel hacking, encourage guests to use virtual private networks (VPN) if they plan on conducting business with sensitive data.

How we can help

Cyber Attack Readiness

Cyber criminals are attacking your networks, applications and people on a daily basis. Statistically speaking, almost every organization will have an attempted attack made against them, whether they realize it or not. Cyber attack readiness is a fundamental cybersecurity service set for organizations of all sizes.

Risk & Compliance

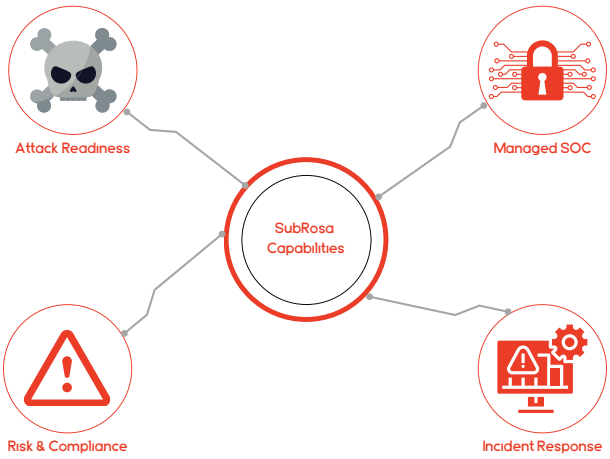
Eliminate holes in your company cyber security defenses to maintain the robustness of your essential information systems, and enhance confidence that your systems and processes address the current risks and industry standards.

Managed Security Operations Center (SOC)

Threat actors don't rest and neither does our managed SOC. Our platform is based on proactive techniques that are built on machine learning, so they are adaptive, constantly improving, and always ready to identify the latest threats.

Incident Response

Security incidents can cripple an organization's operations in a matter of minutes. If an incident is not responded to in a timely, professional manner, costs can spiral and irreparable damage can occur.



More resources available at: https://subrosacyber.com

SubRosa
2000 Auburn Dr
Ste 200 #366
Beachwood OH
44122
888.893.1983
info@subrosacyber.com

Since 2017 SubRosa proudly delivers cyber risk advisory and related services to public, private and government clients.

This brochure is to be used as a reference for general information only, and no content contained herein is designed to provide cyber risk professional advice or services.