TRAVEL WEEKLY
The Travel Industry's Trusted Voice

Hotels

Hotels shown to be susceptible to cybercrime

By Danny King / April 26, 2017

The hospitality industry continues to be a lucrative target for hackers and cybercriminals, the most recent example being a data breach of guests' payment cards at nearly 1,200 InterContinental Hotels Group hotels in the U.S.

The annual cost of payment-card fraud doubled worldwide between 2012 and 2015, to about $22 billion. It is expected to approach $32 billion by 2020, according to the Nilson Report, a newsletter covering the payment systems industry.

The U.S. accounts for almost 40% of those losses and totals about 13 million victims a year.

Some of the higher-profile payment-card breaches in recent years include Target, which said that data from as many as 70 million people had been compromised by a breach in 2013, and Home Depot, which the following year estimated that information had been stolen from as many as 56 million customers.

As for the hotel industry, Hilton, Hyatt and Starwood have reported data breaches at hotels since 2015.

Brian Krebs, a Virginia-based writer of the KrebsOnSecurity cybersecurity blog, said, "I'd be surprised if there was a credit card used at a hotel within the last year where it wasn't somehow compromised."

From a legal standpoint, experts said that IHG is not directly liable for the breach because it occurred at independently owned and operated franchise properties, not through IHG's global reservation system. Still, Ashton Mozano, chief technology officer at Boulder, Colo.-based cybersecurity software maker Circadence, said the hotelier's reputation will take a hit because travelers associate the breach with the brand parent.

Additionally, Mozano said, the breach illustrates how franchise hotels, especially those in the lower end of price spectrum, are particularly susceptible to cybercrime. About 70% of IHG's hotels are franchised.

About 770 Holiday Inn Express, 180 Holiday Inn, 120 Candlewood Suites and 50 Staybridge Suites hotels were affected by the IHG breach. No data breach was detected at an InterContinental or Kimpton hotel.

"The upper-scale companies used to be a perfect place to attack, but I've seen massive improvement," Mozano said. He added that at lower-price hotels, "there are a lot of people in management positions or franchise owners who just don't realize or appreciate the level of vulnerability that they could be exposed to."

IHG spokesman Neil Hirsch said IHG hotels that had implemented an IHG encryption payment acceptance

program called Secure Payment Solution (SPS) prior to last Sept. 29 were not impacted by the malware, and hotels that adopted SPS since then were able to put a stop to the malware's security breaches.

Both Krebs and Mozano said that the proliferation of chip-and-pin cards and the resulting growing number of businesses that can process them without a magnetic-card swipe could reduce the frequency of such cyberattacks.

"With a data-chip card, you can't take that data and make it into its own card, or at least not cheaply," said Krebs.

Still, the scale of the IHG breach reflects how many cybercriminals continue to stay a step ahead of both customers and businesses, and some are figuring out ways to pull information off of chip-and-pin cards as well.

"If this was the case in 2001 or 2002, you could understand [the IHG breach]," said Mozano. "But this was 2016. Business owners must be more proactive."

Comments

100 Lighting Way Secaucus, NJ 07094-3626 USA
Telephone: (201) 902-2000